计算机网络安全存在的问题及对策研究

李 可 唐懋钧 陈 鹏 郭珂琦 王 力
北京计算机技术及应用研究所 北京 100854

摘 要：随着信息技术的飞速发展，计算机网络安全问题日益突出。本文深入探讨了计算机网络安全存在的问题，包括技术和管理两个方面的问题。针对这些问题，本文提出了一系列有效的对策，包括加强技术防护、建立完善的安全管理制度、加强用户安全意识教育、加强合作和信息共享等。这些对策可以帮助提高网络安全性，保护用户的信息安全。

关键词：计算机；网络安全；存在问题；对策研究

引言：计算机网络安全问题已经成为当今社会关注的热点问题。随着互联网的普及和信息技术的飞速发展，计算机网络在各个领域得到了广泛应用，深刻地改变了人们的生活和工作方式。然而，网络安全问题也随之凸显出来，个人隐私泄露、企业数据被盗、国家机密被窃等事件频频发生，对个人利益、企业竞争力和国家安全造成了严重威胁。因此，对计算机网络安全存在的问题及对策进行研究具有重要的现实意义和理论价值，是当今社会亟待解决的问题。

1 计算机网络安全的重要性

随着计算机技术和互联网的普及，计算机网络已经深入到人们生活的方方面面，如办公、购物、社交等。在这种情况下，网络安全问题变得越来越重要。计算机网络涉及到大量的个人信息、企业数据和国家机密等敏感信息，一旦遭到攻击或泄露，将对个人隐私和企业利益造成严重威胁，甚至影响到国家安全。其次，计算机网络是一个复杂的系统，涉及到硬件、软件、协议等多个方面，容易受到各种形式的攻击和威胁。例如，黑客可以利用漏洞进行入侵、窃取数据或破坏系统；病毒和恶意软件可以感染和传播，导致系统崩溃或数据丢失；拒绝服务攻击可以导致网络瘫痪等。这些攻击和威胁不仅会影响网络的正常运行，还会给用户带来巨大的经济损失和精神负担[1]。最后，计算机网络安全不仅是一个技术问题，更是一个涉及到法律、道德和社会责任等方面的问题。国家和企业应该制定和执行相关的法律法规和技术标准，加强网络安全教育和培训，提高公众的网络安全意识和技能。同时，企业和个人也应该承担起相应的责任和义务，加强自身的网络安全防护和管理，共同维护一个安全、稳定、可靠的计算机网络环境。

2 计算机网络安全存在的主要问题

2.1 网络通信安全问题

网络通信安全问题是一个复杂且重要的问题，它涉及到网络通信过程中数据的传输安全和保密问题。随着互联网的普及和网络技术的发展，网络通信已经成为了人们日常生活中的重要组成部分，因此，保障网络通信的安全性对于个人隐私和企业机密都具有重要意义。数据窃取是网络通信安全问题中最常见的一种。攻击者可以利用各种手段，如截获、监听、分析等，获取网络中传输的数据，从而获取敏感信息。数据窃取不仅会影响个人隐私和企业机密的安全性，还可能被用于进行欺诈、恶意攻击等行为。数据篡改是指攻击者对网络中传输的数据进行篡改或注入恶意数据，导致数据的不完整或错误。数据篡改可能导致各种问题，如信息误导、数据损坏、系统崩溃等。假冒身份是指攻击者通过伪装成合法的用户或系统，进行网络通信和操作。假冒身份可能导致敏感信息的泄露、未经授权的访问和操作等。

2.2 操作系统安全问题

操作系统作为计算机网络的基础软件环境，具有至关重要的作用。然而，由于操作系统设计的复杂性和庞大的代码量，很难保证没有任何漏洞或缺陷。因此，操作系统安全问题主要是由系统漏洞引起的。系统漏洞是指操作系统中存在的安全缺陷或漏洞，这些漏洞可能被攻击者利用，从而获取系统的控制权或窃取敏感信息。系统漏洞的产生可能是由于操作系统设计时的缺陷、编程语言的局限性、软件工程的错误等原因造成的。恶意软件是指故意在计算机系统中安装后门、收集用户信息的软件。恶意软件主要包括病毒、蠕虫、特洛伊木马等，它们可以通过网络、邮件等方式传播，对操作系统造成严重的安全威胁[2]。病毒是一种常见的恶意软件，它可以在计算机系统中自我复制并传播，同时破坏系统文件、占用系统资源、干扰系统运行等。病毒可以通过网络、移动存储设备等方式传播，对操作系统安全构成严

重威胁。

2.3 应用软件安全问题

应用软件是计算机网络中用于实现特定功能和服务的软件，其安全性对于整个网络的安全至关重要。然而，由于软件设计和开发过程中的一些问题，应用软件可能会出现各种安全漏洞，从而给攻击者提供可乘之机。缓冲区溢出是一种常见的应用软件安全问题。在软件开发过程中，如果对缓冲区的长度或大小没有进行正确的处理和验证，就可能导致缓冲区溢出。攻击者可以利用缓冲区溢出漏洞，向缓冲区中注入恶意代码，从而控制程序的执行流程，窃取敏感信息或进行其他恶意操作。格式化字符串攻击也是一种常见的应用软件安全问题。在C和C++等编程语言中，格式化字符串函数用于将格式化的数据写入字符串中。如果程序员没有正确处理格式化字符串中的控制字符，就可能导致格式化字符串攻击。攻击者可以利用格式化字符串漏洞，向程序中注入恶意代码或参数，从而控制程序的执行流程或获取敏感信息。

2.4 管理安全问题

管理作为计算机网络安全的重要环节，对于整个网络的安全性起着至关重要的作用。然而，由于管理涉及到多个方面和复杂的因素，因此也最容易被忽视。管理安全问题主要是由于管理制度和管理手段的不完善和不到位所引起的，这在一定程度上导致了网络安全问题的发生。管理制度不健全是管理安全问题的主要原因。很多组织和企业缺乏完善的网络安全管理制度，或者制度内容过于简单、不够具体，导致管理人员在执行过程中无法全面、准确地遵循。此外，制度的更新和修订也不够及时，无法跟上网络安全形势的变化，从而导致了安全漏洞和风险的出现。管理手段不严格也是管理安全问题的一个重要原因。由于缺乏有效的管理手段或工具，管理人员很难对网络安全进行全面、细致的管理。例如，对网络设备和系统的监控、日志分析、访问控制等管理手段的不到位，都可能导致网络安全问题的发生。此外，管理人员的技术水平和安全意识也是影响管理效果的重要因素。

3 计算机网络安全的对策研究

3.1 建立完善的网络安全管理制度

建立完善的网络安全管理制度是保障计算机网络安全的基石。一个健全的网络安全管理制度应该包括安全审计制度、应急响应制度、安全培训制度等多个方面，以确保网络安全管理的全面性和有效性。安全审计制度是网络安全管理制度的重要组成部分。通过建立安全审计制度，可以对网络系统和应用程序进行全面的安全审查和监控，及时发现和修复安全漏洞。同时，安全审计制度还可以对网络行为进行记录和分析，为后续的安全事件调查提供依据。具体来说，安全审计制度需要明确审计范围、审计内容、审计方法和审计程序等，并要求相关人员严格遵守。通过定期和不定期的安全审计，及时发现安全问题，采取相应的措施加以解决，确保网络系统的安全性。应急响应制度是网络安全管理制度的重要环节。在网络安全事件发生时，应急响应制度可以迅速启动，协调各方资源，进行及时有效的应急处置。应急响应制度应该包括应急响应流程、处置方案、技术支援等多个方面，确保在安全事件发生时能够迅速应对。

3.2 加强网络安全技术防护

加强网络安全技术防护是保障计算机网络安全的必要手段。为了有效地防止网络攻击和数据泄露，需要采用多种网络安全技术手段，包括防火墙、入侵检测系统、加密技术等。防火墙是网络安全技术防护的重要手段。通过设置防火墙，可以有效地隔离内部网络和外部网络，防止未经授权的访问和数据泄露[3]。同时，防火墙还可以对网络流量进行监控和过滤，防止恶意软件的传播和攻击。在选择和使用防火墙时，需要根据实际情况进行配置和管理，确保其能够有效地保护网络的安全性。入侵检测系统是另一种重要的网络安全技术防护手段。入侵检测系统可以对网络流量进行实时监测和分析，发现异常行为和攻击行为，并及时采取相应的措施进行防范和应对。通过与防火墙的配合使用，可以更全面地保障网络的安全性。加密技术是保障数据传输和存储安全的另一种重要手段。通过对数据进行加密处理，可以有效地防止数据被窃取或篡改。在数据传输过程中，可以采用传输层加密技术，如SSL/TLS等，对数据进行加密传输；在数据存储时，可以采用存储加密技术，如全盘加密、文件加密等，对数据进行加密存储。

3.3 定期进行安全漏洞检测和修复

定期进行安全漏洞检测和修复是保障计算机网络安全的必要措施。安全漏洞是网络系统中最常见的安全问题，如果不及时发现和修复，可能会导致严重的安全事件，如数据泄露、系统瘫痪等。首先，安全漏洞检测是发现安全漏洞的重要手段。通过对网络系统进行全面的扫描和测试，可以发现潜在的安全漏洞和隐患。常用的安全漏洞检测方法包括漏洞扫描、渗透测试和源代码审查等。这些方法可以帮助发现各种类型的安全漏洞，如缓冲区溢出、跨站脚本攻击等。在选择和使用安全漏洞检测方法时，需要根据实际情况进行选择和配置，确保

能够全面地检测到网络系统中的安全漏洞。其次，修复安全漏洞是保障网络安全的重要环节。一旦发现安全漏洞，需要及时采取相应的措施进行修复和解决。对于一些常见的安全漏洞，可以通过更新软件版本、配置安全策略等方式进行修复。在修复安全漏洞时，需要确保修复措施的有效性和安全性，避免产生新的安全问题。最后，需要强调的是，定期进行安全漏洞检测和修复是一项持续性的工作。网络安全是一个不断变化的领域，新的安全漏洞和攻击手段不断出现。

3.4 建立备份和恢复机制

建立备份和恢复机制是保障计算机网络安全的必要措施。在网络安全事件频发的今天，数据和系统的安全性至关重要。首先，对重要数据和系统进行备份是备份和恢复机制的基础。备份的目的是为了在数据丢失或系统故障时能够快速恢复到正常状态。在选择备份方式时，需要根据实际情况进行选择和配置，如全量备份、增量备份等。其次，建立恢复机制是备份和恢复机制的重要环节。恢复机制的目的是为了在数据丢失或系统故障时能够快速恢复到正常状态。因此，需要制定详细的恢复计划和流程，明确恢复责任人和恢复流程等。同时，还需要定期进行恢复演练和测试，确保恢复计划的有效性和可行性。在恢复过程中，还需要注意数据的一致性和完整性，避免数据损坏或丢失。最后，需要强调的是，建立备份和恢复机制是一项持续性的工作[4]。网络安全是一个不断变化的领域，新的攻击手段和故障不断出现。因此，需要定期对备份和恢复机制进行评估和更新，确保其能够适应新的安全威胁和变化。只有这样，才能保障计算机网络的安全性，促进经济的持续稳定发展。

3.5 提高用户的安全意识

提高用户的安全意识是保障计算机网络安全的必要措施。用户是网络系统中最薄弱的环节，很多网络安全事件都是由于用户的安全意识不足导致的。因此，提高用户的安全意识对于保障网络安全至关重要。首先，加强用户的安全教育是提高安全意识的基础。通过开展各种形式的安全教育活动，如安全知识讲座、安全培训课程等，向用户普及网络安全知识和技能，提高用户对网络安全的认识和重视程度。这有助于用户更好地理解网络安全的重要性，增强自我保护意识和能力。其次，加强用户的技能培训是提高安全意识的关键。通过培训课程和实践操作，可以帮助用户掌握各种网络安全工具和技能，如密码管理、安全软件使用、安全漏洞修复等。这有助于提高用户的操作能力和应对能力，更好地应对网络安全威胁。最后，建立完善的安全管理制度和流程是提高安全意识的保障。仅仅依靠用户自身的意识和能力是不够的，还需要通过建立完善的安全管理制度和流程来规范用户的行为和操作[5]。这包括制定详细的安全管理制度和流程，如用户账号管理、访问控制等，规范用户的权限和操作方式。同时，还需要建立完善的监督和考核机制，对用户的行为和操作进行监督和评估，确保用户安全意识的有效实施。

结语：综上所述，计算机网络安全是一个复杂而重要的问题，需要各方共同努力来解决。为了保障网络的安全性，我们不仅需要加强技术防护，建立完善的安全管理制度，还需要加强用户安全意识教育，加强合作和信息共享。同时，我们还需要不断地进行技术研究和创新，以应对不断变化的网络安全威胁。希望本文的研究可以为相关领域提供一些有益的参考和启示，推动计算机网络安全研究的进步。

参考文献

[1]蔡海珍.计算机网络安全性维护研究思路构建[J].网络安全技术与应用，2020（11）：5-6.

[2]王立军.计算机网络工程安全防护中存在的问题及解决对策[J].电子技术与软件工程，2019（21）：188-189.

[3]谷允金.计算机网络工程安全存在问题及其对策[J].电子技术与软件工程，2019（19）：192-193.

[4]赵任飞.计算机网络信息安全威胁及数据加密技术探究[J].网络安全技术与应用，2020（11）：40-41

[5]蒋回生.大数据时代计算机网络安全及防范措施研究[J].网络安全技术与应用，2020（11）：71-72.