计算机网络安全存在的问题及对策研究

张一鸣　单齐桓　刘伟隆
北京计算机技术及应用研究所　北京　100054

摘　要：随着信息技术的飞速发展，计算机网络已成为现代社会不可或缺的基础设施，广泛应用于经济、文化、科研、教育、军事及日常生活的各个领域。然而随之而来的网络安全问题也日益凸显，严重威胁着网络系统的稳定性和用户数据的安全性。本文旨在探讨计算机网络安全的重要性，分析当前存在的主要安全问题，并提出相应的解决对策，同时介绍网络安全模型与框架，以期为构建安全、可靠的网络环境提供参考。

关键词：计算机网络安全；问题；对策；模型；框架

引言：在信息化时代，计算机网络作为信息传输和存储的主要载体，其安全性直接关系到国家安全、社会稳定和个人隐私保护。随着网络技术的不断演进，网络安全威胁也日益复杂多变，给网络系统的安全防护带来了巨大挑战。因此深入研究计算机网络安全问题及其对策，对于维护网络空间安全、促进信息化健康发展具有重要意义。

1 计算机网络安全的重要性

在数字化时代，计算机网络安全的重要性如同数字世界的基石，稳固而不可或缺。这一议题不仅关乎技术层面的挑战与应对，更深刻影响着国家安全、社会稳定以及每一个个体的权益与福祉。

1.1 国家安全与政治稳定的基石

计算机网络安全是国家安全的重要组成部分。在信息化高度发达的今天，网络空间已成为国家间竞争与合作的新领域。网络存储和处理的信息中，不乏涉及国家安全战略、军事机密、外交政策等核心领域的内容。一旦这些信息被非法获取或篡改，将直接威胁到国家的安全稳定，甚至可能引发国际争端和冲突。因此，加强计算机网络安全防护，是维护国家主权、安全和发展利益的重要举措。

1.2 经济发展与商业信誉的保障

计算机网络安全对于经济发展和商业信誉具有至关重要的影响。随着电子商务、云计算、大数据等技术的广泛应用，网络已成为企业运营和市场竞争的关键平台。企业的商业机密、客户数据、交易信息等敏感信息均存储在网络中[1]。一旦这些信息泄露或被恶意利用，将给企业带来巨大经济损失，甚至可能导致企业破产倒闭。同时网络安全问题也会严重损害企业的商业信誉和品牌形象，影响其在市场中的竞争力和生存能力。因此，加强计算机网络安全防护，是保障企业经济安全、促进经济持续健康发展的必然要求。

1.3 个人隐私保护与社会稳定的维护

计算机网络安全直接关系到个人隐私保护和社会稳定。在数字化时代，个人生活与网络紧密相连，从社交媒体到在线购物，从电子支付到远程办公，网络已成为人们日常生活中不可或缺的一部分。然而，随着网络应用的普及和深入，个人隐私泄露的风险也日益增加。黑客攻击、病毒传播、网络诈骗等安全威胁层出不穷，严重威胁着个人隐私的安全和权益。此外，网络安全问题还可能引发社会恐慌和不稳定因素，如谣言传播、网络暴力等。因此，加强计算机网络安全防护，是保护个人隐私、维护社会稳定和公共秩序的重要手段。

2 计算机网络安全存在的问题

在数字化浪潮席卷全球的今天，计算机网络安全已成为一个不容忽视的重大议题。随着技术的飞速发展，网络空间日益成为信息交流与资源共享的重要平台，但同时也成为了不法分子窥伺与攻击的温床。当前，计算机网络安全面临着诸多复杂而严峻的问题，这些问题不仅威胁着网络系统的稳定运行，更对国家安全、社会稳定以及个人隐私构成了巨大挑战。

2.1 网络攻击手段多样且隐蔽性强

网络攻击是计算机网络安全面临的首要威胁。攻击者利用先进的技术手段，设计出各种隐蔽性强、破坏力大的攻击方式，如病毒、木马、蠕虫等恶意软件的传播，黑客通过漏洞入侵系统窃取数据或破坏关键设施，以及分布式拒绝服务（DDoS）攻击导致网络服务瘫痪等。这些攻击手段不仅难以防范，而且往往具有高度的隐蔽性，使得受害者在不知不觉中遭受损失。

2.2 软件漏洞和缺陷频发

软件是计算机系统的核心组成部分，其安全性和稳定性直接关系到整个网络系统的安全。然而，由于软件

开发过程中的复杂性、人为失误以及技术限制等因素，软件漏洞和缺陷难以完全避免[2]。这些漏洞和缺陷一旦被攻击者发现并利用，就可能成为其入侵系统的突破口。例如，操作系统、数据库、应用软件等关键组件的漏洞，往往成为黑客攻击的重点目标。此外，随着物联网、云计算等新兴技术的兴起，这些领域的软件安全问题也日益凸显，给网络安全带来了新的挑战。

2.3 内部威胁不容忽视

除了外部攻击外，内部威胁也是计算机网络安全不可忽视的重要因素。内部人员可能出于各种原因，如利益驱动、疏忽大意或恶意破坏等，对网络系统进行非法操作或泄露敏感信息。这种威胁往往更加难以防范，因为内部人员通常具有更高的权限和更深入的了解系统结构。一旦内部人员成为攻击者，其造成的破坏往往更加严重和难以挽回。

2.4 用户安全意识薄弱及管理不善

用户是网络安全的第一道防线，但遗憾的是，许多用户的安全意识仍然相对薄弱。他们可能忽视密码安全、随意点击不明链接、下载未经验证的软件等，这些行为都为攻击者提供了可乘之机。此外，一些组织和企业在网络安全管理方面也存在不足，如缺乏完善的网络安全制度、未定期进行安全培训和演练、对外部设备和人员的接入控制不严等。这些管理上的漏洞也为网络安全带来了潜在的风险。

3 解决计算机网络安全存在问题的对策

3.1 加强技术防护，提升网络安全屏障

（1）强化加密技术应用：加密是保护数据机密性和完整性的重要手段。通过采用先进的加密算法（如AES、RSA等），对敏感数据进行加密处理，即使数据在传输或存储过程中被截获，攻击者也无法轻易解密获取原文。同时加强密钥管理，确保密钥的安全生成、分发、存储和销毁，防止密钥泄露导致的安全风险。（2）部署高效的防火墙和入侵检测系统：防火墙作为网络的第一道防线，能够有效阻止未经授权的访问和恶意流量。应根据实际需求合理配置防火墙规则，并定期更新规则库以应对新出现的威胁。同时部署入侵检测系统（IDS）和入侵防御系统（IPS），对进出网络的数据包进行深度分析，及时发现并阻止潜在的攻击行为。（3）实施身份认证与访问控制：建立完善的身份认证机制，采用多因素认证方式（如密码+手机验证码、生物识别等），提高用户身份验证的准确性和安全性。并且实施严格的访问控制策略，根据用户角色和权限分配相应的资源访问权限，防止未授权访问和内部数据泄露。

3.2 完善管理制度和流程，强化内部控制

（1）制定并执行严格的网络安全规章制度：结合实际情况，制定全面、具体、可行的网络安全规章制度，明确各部门、各岗位的网络安全职责和操作流程[3]。通过定期审计和检查，确保规章制度的得到有效执行，对违规行为进行严肃处理，形成有效的威慑力。（2）加强网络安全培训和教育：将网络安全培训纳入员工日常培训计划，定期组织员工参加网络安全知识培训和应急演练，提高员工的网络安全意识和防范能力。并且建立网络安全文化，鼓励员工积极报告发现的安全问题和隐患，形成全员参与网络安全的良好氛围。（3）定期进行风险评估和漏洞扫描：定期开展网络安全风险评估工作，识别潜在的安全威胁和漏洞。利用专业的漏洞扫描工具对系统进行全面扫描，及时发现并修复安全漏洞。并且对第三方软件和服务进行严格的安全审查，确保其符合网络安全要求。

3.3 提高用户安全意识和管理水平

（1）加强用户教育：通过线上线下相结合的方式，开展网络安全教育活动，向用户普及网络安全知识、常见的网络诈骗手法及防范措施。提高用户对网络安全的认识和重视程度，增强自我保护能力。（2）强化密码管理：引导用户设置复杂且独特的密码，并定期更换密码。同时推广使用密码管理工具或密码本等辅助工具，帮助用户安全地管理和存储密码。（3）警惕钓鱼邮件和恶意链接：教育用户识别钓鱼邮件和恶意链接的特征和手法，不轻易点击来源不明的链接或下载附件。对于疑似钓鱼邮件或恶意链接，应及时向相关部门报告并采取相应措施。

3.4 建立应急响应机制和灾难恢复计划

（1）制定应急响应预案：根据网络安全的实际情况和可能面临的风险，制定详细的应急响应预案。明确应急响应流程、责任分工和处置措施，确保在发生安全事件时能够迅速、有序地应对。（2）定期组织应急演练：通过模拟真实的安全事件场景，定期组织应急演练活动。检验应急响应预案的可行性和有效性，提高应急响应团队的协同作战能力和处置能力。（3）建立灾难恢复计划：制定完善的灾难恢复计划，包括数据备份、系统恢复、业务连续性等方面的内容。确保在发生严重安全事件或灾难性故障时，能够迅速恢复数据、系统和业务运行，减少损失和影响。

4 网络安全模型与框架

在信息化时代，网络安全已成为国家安全、社会稳定和经济发展的重要基石。为了有效应对日益复杂的网

络威胁，构建科学合理的网络安全模型与框架显得尤为重要。这些模型与框架不仅为网络安全工作提供了系统的理论指导，还促进了防护策略、检测技术和应急响应机制的协同发展，从而构建了一个全方位、多层次的网络安全防护体系（如图1）。

图1 网络安全模型与框架示意图

4.1 经典网络安全模型概述

4.1.1 PDR模型

PDR模型，即防护（Protection）、检测（Detection）和响应（Response）模型，是网络安全领域早期的经典模型之一。该模型强调在事前通过加强防护措施来减少安全风险，在事中通过高效的检测手段及时发现并定位威胁，以及在事后通过迅速的响应机制来遏制损害并恢复系统正常运行。PDR模型为网络安全工作提供了一个清晰的框架，有助于实现安全策略的有效落地。

4.1.2 P2DR模型

在PDR模型的基础上，P2DR模型（Policy，Protection，Detection，Response）增加了策略（Policy）这一维度。策略是整个安全体系的核心，它指导着防护、检测和响应等各个环节的实施。P2DR模型强调安全策略的制定应基于风险评估和需求分析，通过动态调整策略来适应不断变化的威胁环境。这种模型使得网络安全工作更加灵活和高效。

4.1.3 PDRR模型

PDRR模型（Protection，Detection，Response，Recovery）在PDR模型的基础上增加了恢复（Recovery）环节[4]。恢复是指在网络系统遭受攻击后，通过备份与恢复技术、应急演练等手段，快速恢复系统正常运行并减少损失。PDRR模型强调了网络安全工作的连续性和可持续性，为应对大规模网络攻击和灾难性事件提供了有力支持。

4.2 新兴网络安全模型探索

4.2.1 APPDRR模型

APPDRR模型（Awareness，Protection，Prevention，Detection，Response，Recovery）在PDRR模型的基础上增加了意识和预防（Awareness，Prevention）两个环节。意识强调提高用户和管理员的安全意识，预防则通过安全培训、安全审计等手段来降低安全事件的发生概率。APPDRR模型更加注重人的因素在网络安全中的作用，有助于构建全员参与的网络安全文化。

4.2.2 PADIMEE模型

PADIMEE模型（Policy，Assessment，Design，Implementation，Monitoring，Evaluation，Education）是一个更加全面和系统的网络安全模型。该模型从政策制定、风险评估、方案设计、实施部署、监控分析、效果评估到教育培训等多个方面入手，构建了一个闭环的网络安全管理体系。PADIMEE模型强调了网络安全工作的持续性和循环性，有助于不断提升网络系统的安全防护能力。

结语

计算机网络安全是信息化时代的重要课题之一。面对日益复杂的网络安全威胁和挑战，我们需要不断加强技术研究和管理创新提高网络安全防护能力。同时加强用户安全意识教育和管理制度建设也是保障网络安全的重要手段。未来随着技术的不断发展和应用场景的不断拓展新的网络安全问题和挑战也将不断涌现。因此我们需要持续关注和研究计算机网络安全问题为推动信息化健康发展贡献力量。

参考文献

[1]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.

[2]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.

[3]范德龙.计算机网络工程安全存在问题及其对策研究[J].通讯世界,2019,26(8):181-182.

[4]魏昌超,冯涛,李兴香,等.机房网络安全隐患及网络安全技术策略研究[J].电子测试,2019(2):132-133.