5G通信时代计算机网络信息安全问题浅析

周　军
华夏邮电咨询监理有限公司　河南　郑州　450007

摘　要：5G是第五代移动通信技术的简称，其应用具有高速率、低时延以及大连接的特点，是最新一代的宽带移动通信技术，5G通信设施是实现人机物互联的网络基础设施。移动通信从1G发展到今天的5G是时代信息技术发展的成果，实现了从语音到数据的转变。在不断的提升中，使得传输速率成倍提升，信息量越来越大反应出来的网络信息安全问题也很突出。

关键词：5G通信；计算机；网络信息；安全问题

1 5G 网络概述

5G网络是第五代移动通信网络的简称，是指第五代移动通信技术。与前几代移动通信技术相比，5G网络具有更高的速率、更低的时延、更大的连接密度和更大的网络容量，可以为用户提供更多、更快、更稳定的通信服务，并实现智能化、物联网和大数据等新一代应用。第一，5G网络具有更高的速率。5G网络在理论上可以实现超过10Gbps的峰值下载速度，是目前4G网络的几十倍。这意味着用户可以更快地下载和上传大容量的数据，无论是观看高清视频、进行在线游戏还是进行高清视频通话，都可以享受到更流畅的体验。第二，5G网络具有更低的时延。延迟是指数据在从发送端到接收端传输过程中的时间间隔，也是衡量通信网络响应速度的重要指标。5G网络的延迟可以低至几毫秒，比4G网络的延迟要低很多。这对于一些对实时性要求较高的应用，如自动驾驶、远程医疗和工业控制等，具有重要意义。除了速度和时延方面的提升，5G网络还具有更大的连接密度和更强的容量。连接密度指的是网络可以同时连接的设备数量，5G网络可以实现每平方公里连接百万级的设备。这为物联网的快速发展提供了基础，使得智能家居、智慧城市和工业自动化等应用得以实现。5G网络也为应用带来了更多的可能性[1]。由于5G网络提供了更高的速度、更低的延迟和更大的容量，为大数据的传输和处理提供了有力支持，使得人工智能、虚拟现实、增强现实等新技术和新应用才得以快速发展。

2 计算机互联网安全的核心隐患

2.1 互联网漏洞

在计算机互联网安全领域，互联网漏洞是一个核心的隐患。互联网漏洞是指计算机互联网系统中存在的安全弱点或缺陷，可能被恶意攻击者利用，从而导致信息泄露、系统瘫痪甚至资产损失等安全问题。互联网漏洞存在的原因有多种，其中包括软件开发过程中的疏忽、设计缺陷、配置错误等。当攻击者发现并利用这些漏洞时，可能会进行各种攻击行为，如黑客攻击、病毒传播、网络钓鱼等，从而危害网络安全。常见的互联网漏洞包括但不限于：代码注入漏洞、跨站点脚本攻击漏洞、跨站点请求伪造漏洞、命令注入漏洞、信息泄露漏洞等。这些漏洞可能会导致被攻击系统的敏感信息被盗取，用户隐私被泄露，系统被入侵控制等严重后果[2]。

2.2 黑客攻击与入侵

在计算机互联网安全领域，黑客攻击与入侵是一个核心的隐患。黑客攻击和入侵指的是未经授权的、恶意的访问和入侵计算机系统或网络的行为，其目的通常是获取敏感信息、破坏系统功能、盗取资产或传播恶意软件等。黑客攻击和入侵的方式多种多样，常见的包括但不限于以下几种：（1）网络扫描和侦察：黑客通过扫描网络、收集目标系统信息，寻找系统漏洞和弱点，为后续攻击做准备。（2）病毒和恶意软件：黑客通过传播病毒、木马、间谍软件和勒索软件等恶意软件，获取用户敏感信息、控制系统或勒索资金。（3）社交工程和钓鱼攻击：黑客利用社交工程手段，通过虚假网站、电子邮件或短信等方式诱导用户点击恶意链接或提供个人敏感信息[3]。（4）拒绝服务攻击：黑客通过发送大量攻击请求，占用系统资源或使系统崩溃，导致目标网络无法正常工作。（5）字典攻击和暴力破解：黑客使用自动化程序和暴力破解工具，尝试使用常见密码、弱密码或穷举法猜测密码，以获取系统权限。

2.3 病毒入侵

在计算机互联网安全领域，病毒入侵是一个核心的隐患。病毒入侵指的是恶意软件（病毒）通过感染计算机系统或网络，对系统造成破坏、盗取信息、控制系统或传播恶意软件等潜在威胁。病毒入侵的方式多种多

样，可以通过电子邮件附件、下载的文件、植入的广告等途径传播。一旦计算机感染了病毒，它可能会对系统功能造成损害，如删除或修改文件、破坏硬件设备等[4]。更严重的是，病毒也可能盗取用户的敏感信息，包括银行账号、密码和个人身份信息等，给用户带来重大的财产和个人隐私损失。

3 5G 通信网络安全分类和采取的主要措施

3.1 虚拟化/软件安全

在5G通信网络中，安全分类主要包括网络安全、信息安全和设备安全三个方面。为了确保5G通信网络的安全性，采取了一系列主要措施，其中虚拟化和软件安全是关键措施之一。首先，虚拟化技术在5G通信网络中起着重要作用。通过虚拟化可以将网络资源划分为独立的虚拟网络，每个虚拟网络都拥有独立的隔离环境和安全策略，从而有效防止病毒和恶意软件的传播，提高网络整体的安全性。其次，软件安全也是确保5G通信网络安全的关键措施之一。在软件开发过程中，需要采取安全编码规范，遵循安全开发流程，以减少安全漏洞的产生。开发人员需要进行代码审查和漏洞扫描，并及时修复潜在的安全问题。另外，5G通信网络还采取了其他措施以保障安全性：（1）访问控制：通过合理的访问控制策略，限制用户和设备的访问权限，确保只有经过授权的用户和设备才能访问网络资源[5]。（2）数据加密：使用强大的加密算法对敏感数据进行加密，确保数据在传输和存储过程中的安全性，只有授权的用户才能解密和访问数据。（3）安全认证：采用多因素身份认证机制，结合密码、生物特征、物理密钥等多个验证因素来确认用户身份，防止非法用户的入侵。（4）安全监控和检测：建立完善的安全监控和检测系统，实时监测网络中的异常行为和潜在的安全威胁，及时发现并应对安全漏洞和攻击事件。

3.2 完善5G安全通信技术体系的构建

为了完善5G安全通信技术体系，我们需要采取一系列措施来构建一个安全可靠的网络。（1）加强网络边界安全：建立高效的防火墙和入侵检测系统，对来自外部网络的攻击进行监测和阻止。确保网络边界的安全，防止未经授权的访问和数据泄露。（2）强化用户身份认证：采用多因素身份认证机制，如密码、生物特征、物理密钥等，以确保用户身份的真实性和合法性。防止非法用户的入侵和身份伪造。（3）建立安全的密钥管理机制：为数据传输过程中的加密和解密建立安全可靠的密钥管理方式。确保通信内容的机密性和完整性[6]。（4）加强虚拟化技术的安全性：通过安全的虚拟化技术，将网络资源划分为独立的虚拟网络，实现资源隔离和安全策略的隔离。防止恶意软件的传播和攻击范围的扩散。（5）配备强大的安全设备和软件：使用经过认证的安全设备和软件，如防火墙、入侵检测系统、加密模块等，以提供更高的安全防护能力。（6）实施安全管理和策略：建立全面的安全管理和策略体系，包括安全漏洞管理、事件响应、持续的安全培训和意识提升等。确保安全措施的落实和持续改进。（7）加强跨部门合作和信息共享：促进政府、企业和学术界之间的合作与信息共享，加强对于网络安全威胁的共同应对。（8）强化安全审计和监测：建立健全的安全审计和监测机制，对网络流量、系统日志和安全事件进行实时的监测和分析。及时发现异常行为和安全威胁，并采取相应措施进行处置[1]。（9）持续关注和应对新威胁：紧密关注最新的威胁和攻击手段，并针对新威胁采取相应的应对措施。定期进行安全评估和渗透测试，发现和修复漏洞，保持系统的安全性和稳定性。

3.3 优化5G安全数据防护系统的升级

为了优化5G安全数据防护系统的升级，我们可以采取以下措施：使用更强大、更安全的数据加密算法和密钥管理机制，确保数据在传输和存储过程中的安全性和机密性。采用最先进的加密算法，如AES-256，以保护敏感数据。建立严格的访问控制策略，根据用户的权限和身份设置细粒度的访问控制。采用基于角色的访问控制（RBAC），确保只有经过授权的用户可以访问相应的数据。建立全面的安全审计和监测机制，对数据传输和访问进行实时监测和分析。通过监测数据流量、访问日志和事件日志，及时发现异常行为和安全威胁，并采取相应措施进行处置。建立规范的漏洞管理机制，及时修复已知的安全漏洞，并定期进行安全评估和渗透测试，发现和修复潜在的漏洞。保持系统的安全性和稳定性[2]。与相关机构和组织建立紧密的合作关系，获取最新的威胁情报和安全漏洞信息。通过共享情报，及时应对新威胁和攻击，提高系统的安全防护能力。加强用户培训和教育，提高用户对安全风险和安全最佳实践的认识。通过合理的权限管理和安全策略，引导用户正确使用和保护数据。制定完善的灾备和恢复计划，确保在发生安全事件或灾难时的快速响应和恢复。备份重要数据，建立冗余系统，以应对各种安全风险和可用性问题。紧密关注最新的安全技术发展和趋势，及时引入新的安全防护技术和工具。利用人工智能和机器学习等技术，提高威胁检测和响应的准确性和效率。

3.4 全方位强化网络监督管理

为了全方位强化网络监督管理，我们需要采取一系

列措施，以确保网络的安全性和稳定性。第一，加强网络监控和分析能力。建立高效的网络监控系统，监测网络流量和活动，及时发现异常行为和安全威胁。通过实时分析和处理网络数据，提高对网络问题和攻击事件的响应速度和准确性。第二，加强网络安全事件的处置和应急响应能力。建立完善的网络安全事件处置机制，制定相关的应急响应计划，并进行定期演练和培训。针对网络攻击和威胁，采取及时有效的措施进行处置和修复，最大程度地减小安全事件的影响[3]。第三，强化网络许可和认证制度。加强对网络服务提供商和相关企业的许可和认证管理，确保其具备必要的能力和安全措施。通过合规性审查和监管，提高网络服务提供商的安全意识和能力，保障用户的信息安全。此外，全方位强化网络监督管理还包括以下措施：（1）制定和完善网络安全法律法规，建立健全的网络安全管理体系，明确相关责任和义务，加强对违法行为的打击和惩处。（2）加强对网络平台和应用的监管。规范网络平台的经营行为，确保其内容合法合规。加强对网络应用程序的审核和监管，防止恶意软件和病毒的传播。（3）强化网络数据保护。加强对个人信息的保护，规范个人信息的收集、使用和存储。加强对企业数据安全的监管，防止数据泄露和滥用。（4）加强对网络基础设施和关键信息系统的安全监控和保护。建立网络基础设施的安全评估和监控机制，保障国家和重要部门的关键信息系统的安全运行。（5）加大网络安全宣传和教育力度。加强网络安全意识教育，提高公众对网络安全问题的认识和防范意识[4]。

3.5 加强5G时代计算机网络信息安全培训

为了加强5G时代计算机网络信息安全，我们需要加强相关培训，提高人员的安全意识和技能。首先，建立全面且系统的信息安全培训计划。制定培训课程，包括网络基础知识、网络安全漏洞与攻击、密码学和加密技术、网络安全事件的响应与处置等内容，确保培训的全面性和针对性。其次，针对不同层次和岗位的人员，开展针对性的培训。对管理人员、技术人员和普通员工进行不同层次的培训，使他们能够全面了解网络安全风险和防护措施，并具备相关的技术和技能。第三，采用多种培训形式和手段。除了传统的面对面培训外，还可以采用在线培训、模拟演练等形式，提高培训的覆盖面和灵活性。还可以通过定期组织网络安全竞赛和演练，提高学习的参与度和实践能力[5]。

结束语

5G通信时代给计算机网络的信息安全提出了新的挑战，但同时也提供了更多的安全保护措施的可能。我们需要认识到信息安全的重要性，并采取相应的措施来应对潜在的安全威胁。只有通过加强网络加密、完善访问控制、强化安全培训等措施，我们才能够在5G时代构建一个安全、稳定的计算机网络环境，为各类用户提供可靠、安全的通信服务。

参考文献

[1]朱君，胡淼.网络时代视角下网络通信安全问题的内外部原因及防范手段[J].现代工业经济和信息化，2022，12(01):121-122.

[2]徐晓建.计算机控制系统中网络通信安全问题探究[J].东西南北，2022(23)：173.

[3]刘楝,孟宪民,李阳.5G安全及网络监管问题探析[J].国防科技，2020(03)：76-79+85.

[4]覃德泽,李立信,李立礼.5G背景下高校信息安全风险分析及防范策略[J].网络安全技术与应用,2020(08):93-94.

[5]陈云杰,游伟.5G移动通信中基于安全信任的网络切片部署策略研究[J].通信技术,2020,53(9):2206-2209.

[6]孟驰.5G移动通信网络安全的探讨[J].数字通信世界,2020(3):145.