计算机网络信息安全及其防护对策研究

钟巧燕

（滁州市机电工程学校，安徽省滁州市，239000）

摘要　计算机网络信息安全作为一个重要的研究领域，一直受到广泛关注。随着技术的进步和网络环境的变化，信息安全形势仍然在不断演变。新兴技术如物联网、云计算和人工智能等给信息安全带来了新的挑战。因此，持续的研究和创新是必要的，这样可以保护计算机网络中的信息安全，并及时应对新的威胁和风险。本文就计算机网络信息安全的重要性和背景进行介绍，并对计算机网络信息安全的基本概念和原理进行阐述，分析了常见的网络攻击手段以及网络安全防护技术。

关键词　计算机；网络信息安全；威胁；防护

中图分类号：TP393　文献标识码：B

文章编号：1008-0899(2024)10-0039-02

随着网络技术的快速发展和信息交流的增加，计算机网络面临着日益严峻的安全威胁和挑战。网络黑客、计算机病毒、网络钓鱼等安全攻击事件频频发生，给个人、企业和国家的信息资产造成了严重损失和影响。

1　计算机网络信息安全的重要性和背景

计算机网络中存在各种潜在的威胁和风险，如黑客攻击、病毒感染、数据泄露等对个人、组织和整个社会造成了巨大的危害，了解和传授计算机网络信息安全的重要性对于学生的综合素质培养非常关键。

计算机网络信息安全是保护个人隐私和财产安全的重要保障。在互联网时代，个人隐私成了一个非常敏感的问题，个人的身份信息、财务信息、健康信息等都储存在计算机网络中。如果这些信息被黑客或其他恶意人员获取并滥用，将会给个人带来巨大的损失和痛苦。

现代国家的政府机构、军事机构、金融机构等都依赖于计算机网络进行信息交流和管理。如果这些关键部门的计算机网络受到攻击或被侵入，将会导致国家机密泄露、军事行动受阻、金融体系瘫痪，对国家的安全和经济发展造成巨大影响[1]。同时，现代社会也高度依赖于计算机网络的运行，包括电力供应、交通管理、医疗保健、公共安全等方方面面。如果计算机网络被攻击导致这些关键基础设施无法正常运行，将会给社会带来混乱和危险。

2　计算机网络信息安全的基本概念

2.1　计算机网络信息安全的基本概念

2.1.1　机密性

机密性是指只有授权用户才能够查看或访问所需的信息。保护机密性需要采用加密技术、访问控制等措施，以确保信息不被未经授权的人员获取[2]。

2.1.2　完整性

完整性是指数据在传输过程中没有被篡改或损坏，并且数据的内容和格式符合预期。保护完整性需要采用数字签名、数据加密和完整性校验等技术，以防止数据在传输过程中被修改或损坏。

2.1.3　可用性

可用性是指可以及时地访问、使用和操作计算机系统和网络。保护可用性需要采用负载均衡、备份和恢复等措施，以确保计算机系统和网络始终处于可用状态。

2.1.4　不可抵赖性

不可抵赖性是指在交换信息的过程中，发送方和接收方都不能否认它们的行为或信息传输的事实。保护不可抵赖性需要采用数字证书、时间戳等技术，以证明信息的真实性和可信性。

2.2　网络攻击手段

网络安全威胁常见类型包括恶意软件和病毒、

作者简介：钟巧燕（1985~），女，汉族，安徽滁州人，本科，讲师，研究方向：计算机。

社交工程攻击、DDoS攻击、零日漏洞利用等，这些威胁和挑战可能造成对网络安全造成严重危害[3]，必须加强网络防范意识。

3 计算机网络信息安全的防护技术

3.1 网络安全防护技术

3.1.1 防火墙

防火墙用于监视和控制进出网络的流量，工作原理是根据预先设定的规则集来检查数据包，并根据规则允许或阻止流量通过。防火墙可以过滤入站和出站流量，提供对网络流量的精细控制和管理，也可以实施访问控制策略，例如基于源IP地址、目标端口、协议类型等进行限制和过滤。防火墙还提供网络地址转换功能，隐藏内部网络拓扑结构。其可以防止常见的攻击，如拒绝服务攻击、端口扫描等。防火墙技术易于实施且成本相对较低，能够提供基本的网络访问控制和保护，可以有效防止一些已知的攻击和恶意流量。防火墙是保护计算机网络免受网络攻击和威胁的重要安全手段，应定期更新防火墙软件和固件，进行安全审计和漏洞扫描，并加强师生的网络安全意识教育。

3.1.2 加密算法

加密通信是通过使用密码算法对数据进行加密，以防止未经授权的访问者窃取或篡改数据。其主要原理是在发送方对数据进行加密，然后在接收方对密文进行解密，只有持有正确密钥的人才能成功解密。加密通信可以确保数据的保密性，用于保护敏感信息，如用户凭据、财务数据等，加密通信支持多种加密算法和协议，如对称加密、非对称加密和传输层安全协议。加密通信为网络通信提供了强大的数据保护，确保数据在传输过程中不被泄露或篡改，其可以适用于各种网络通信环境，包括互联网、局域网等。在加密算法教学中，应注重理论知识和实践操作相结合，帮助学生深入理解加密算法的原理和应用。此外，还应强调加密算法在保护个人隐私和敏感数据方面的重要性，提高学生对网络安全的认识和意识。

3.2 安全策略的制定和实施

3.2.1 安全策略和访问控制

安全策略可以通过制定和执行各种安全策略来防御威胁并减轻潜在风险，访问控制用于验证和控制用户或实体对系统和数据的访问权限。安全策略涵盖了多个方面，包括网络安全、数据安全、身份验证、访问控制等，可以根据具体需求和威胁环境进行定制，以满足不同组织和系统的安全需求。访问控制包括认证、授权和审计三个基本步骤，以确保只有合法用户可以访问资源，访问控制可以根据不同级别的安全需求进行细分，如物理访问控制、逻辑访问控制等。访问控制支持集中式管理和控制，便于管理和维护访问控制策略。

3.2.2 网络监控与日志记录

使用网络流量分析工具（如Wireshark、Snort）对网络流量进行实时监测和分析，以检测异常活动和潜在威胁。同时，部署IDS来检测并警报可能存在的入侵行为，如异常的数据包、恶意软件传播等。IDS可以基于特定规则进行检测，也可以采用机器学习等技术进行行为分析。此外，也要进行审计日志的监控，监控关键系统和应用程序的审计日志，以及网络设备（如防火墙、路由器）的日志，及时发现异常事件和安全事件。

日志记录是非常重要的网络监管手段。启用操作系统、应用程序以及网络设备的日志功能，并配置适当的日志记录级别，将关键事件和操作记录到日志中。日志内容应包括登录尝试、文件访问、异常行为等。同时，建立中央化的日志管理系统，将不同设备、应用程序的日志集中存储和管理。

4 结语

随着计算机网络的广泛应用和信息技术的迅猛发展，信息安全问题日益突出。需要持续关注计算机网络信息安全领域的最新动态，并不断加强安全意识和技术能力，以应对不断变化的安全威胁。

参考文献

[1] 马玥桓.计算机网络信息安全及其防护对策探讨[J].现代信息科技,2022,6(19):116-119.

[2] 李效渊,刘赛彬.计算机网络信息安全及其防护对策探析[J].无线互联科技,2021,18(10):83-84.

[3] 赵丹耀.基于计算机网络信息安全及其防护对策研究[J].中国多媒体与网络教学学报(上旬刊),2020(06):247-248.