计算机网络安全技术的影响因素与防范措施

陈春梅
重庆信科设计有限公司　重庆　400000

摘　要：计算机网络安全技术在当今信息时代的发展中扮演着至关重要的角色。随着互联网的普及和依赖程度的增加，网络安全问题也愈发凸显。了解计算机网络安全技术的影响因素以及相应的防范措施，对于确保我们的信息和资产的安全具有重要意义。本文将详细介绍计算机网络安全技术的影响因素，并提供一些常用的防范措施。

关键词：计算机网络；安全技术；影响因素；防范措施

引言

随着计算机网络的快速发展和广泛应用，网络安全问题变得日益突出。计算机网络安全技术的影响因素涉及各种恶意软件攻击、网络钓鱼、拒绝服务攻击、数据泄露、身份欺骗以及网络间谍活动等。为了应对这些威胁，采取相应的防范措施至关重要。防火墙、入侵检测系统和入侵防御系统、数据加密以及强密码策略等是常见的防范手段。本文将详细探讨这些影响因素，并提供一些有效的防范措施，以确保计算机网络的安全性与稳定性。

1 计算机网络安全技术的影响因素

1.1 恶意软件攻击

恶意软件是指故意编写并传播的恶意程序，包括病毒、蠕虫、木马等。这些恶意软件可以通过感染用户设备或网络系统来窃取个人信息、损坏数据或控制系统。首先，病毒和蠕虫可以自我复制并传播到其他设备或系统中，导致大规模的感染，从而造成严重的网络瘫痪或数据泄露。木马程序可以悄无声息地植入系统中，并在背后进行各种非法操作，例如窃取密码、监视用户活动或发起网络攻击。其次，通过感染恶意软件，黑客可以窃取个人敏感信息，如银行账号、信用卡信息、登录凭证等。这些信息可以被用于盗取身份、进行欺诈活动或者散布虚假信息，给个人和组织带来严重的财务损失和声誉损害。此外，恶意软件攻击还可以导致数据的损坏或丧失。某些恶意软件会删除或篡改用户的数据，造成不可逆转的损失。对于企业和组织来说，数据丢失可能导致生产中断、财务损失或法律责任。

1.2 网络钓鱼

网络钓鱼指的是攻击者冒充合法实体，通过发送虚假的电子邮件或网页来欺骗用户输入敏感信息，如用户名、密码、信用卡号码等。网络钓鱼攻击往往利用社交工程学的技巧来骗取用户的信任。攻击者通过伪装成合法的组织、企业或个人，发送看似真实的电子邮件或网页链接给用户，诱使他们点击链接并在虚假的页面上输入敏感信息。这些邮件或网页通常采用合理的语言、逼真的设计和合法的标志，以增加用户被欺骗的可能性[1]。网络钓鱼攻击是一种欺骗性手段，通过冒充合法实体来获取用户的敏感信息。其次，攻击者使用的技术和手法不断变化，以适应不同的网络环境和用户行为。再次，网络钓鱼攻击泛滥成灾，威胁着用户的隐私和财产安全。网络钓鱼攻击可以导致用户的个人信息被盗取、账户被盗用，甚至导致财务损失。此外，网络钓鱼攻击还可能给企业和组织带来声誉损失和经济损失。

1.3 拒绝服务攻击

拒绝服务攻击的目标是通过发送大量请求来使目标系统或网络变得不可用。攻击者会利用各种手段，如TCP/IP协议漏洞、资源耗尽或错误配置等，向目标系统发送大量的恶意请求。DoS攻击可以采取多种形式，包括TCP SYN洪水攻击、UDP洪水攻击、ICMP洪水攻击和HTTP GET/POST洪水攻击等。攻击者通过发送大量的请求，消耗目标系统的带宽、处理能力和存储空间，导致系统无法正常运行或崩溃。随着技术的不断发展，拒绝服务攻击也在不断演化。分布式拒绝服务攻击是一种更为复杂和具有威胁性的攻击形式。DDoS攻击利用多个来源的攻击者同时向目标系统发动攻击，使得攻击的规模更大，难以抵御和追踪攻击源。拒绝服务攻击对计算机网络安全产生了严重的影响。首先，它削弱了网络的可用性，使得合法用户无法正常访问系统或服务。其次，攻击可能导致系统崩溃、数据丢失和业务中断，对组织的运营造成重大影响[2]。此外，拒绝服务攻击还可以作为干扰竞争对手的一种手段，用于攻击特定的组织或个人，损害其声誉和利益。

1.4 数据泄露

数据泄露指的是未经授权地披露敏感信息，可能由于安全漏洞、恶意内部人员的行为、雇员失误等原因导

致。数据泄露对个人隐私和企业声誉造成严重威胁。首先，当个人敏感信息被泄露后，个人的隐私将面临被滥用、冒用甚至盗用的风险。例如，身份证号码、银行账户信息、医疗记录等都可能被黑客获取并用于不法目的，给个人带来财务损失和精神困扰。其次，数据泄露会对企业的声誉和信任度造成严重打击。一旦敏感商业数据或客户资料遭到泄露，企业可能面临巨额经济损失，同时也会失去客户的信任与支持。大规模的数据泄露还可能对整个市场产生负面影响，引发社会公众的关注和担忧，从而进一步削弱企业的地位和市场竞争力。此外，数据泄露还会引发法律和合规问题。对于一些行业来说，如医疗、金融等，数据泄露的后果可能更为严重，因为这些行业处理的是涉及个人敏感信息的大量数据。

1.5 网络间谍活动

网络间谍活动往往涉及国家安全和商业竞争等重要领域，对于个人、组织和国家来说都具有严重的影响。首先，攻击者可以通过黑客手段入侵个人电脑、智能手机等设备，窃取个人敏感信息，例如银行账号、身份证号码、社交媒体账号等。这些信息被盗取后可能被不法分子用于犯罪活动，给个人造成财产损失和心理困扰[3]。其次，攻击者可能通过渗透目标企业的网络系统，获取商业机密、研发资料、客户数据等重要信息，从而导致商业机密泄露、产品仿制、商业间谍行为等，给企业带来巨大经济损失。这种活动尤其在跨国公司之间的竞争中更加常见，对企业的竞争力和市场地位造成直接影响。此外，网络间谍活动还涉及国家安全问题。攻击者可以通过渗透政府机构、军事系统等重要网络设施，窃取国家机密、军事情报以及关键基础设施的信息。这对于国家的安全和利益构成了巨大威胁，可能导致政治、经济、社会稳定等方面的严重后果。

2 计算机网络安全技术的防范措施

2.1 防火墙

防火墙是位于网络边界，负责监控和控制进出网络的流量。防火墙通过设定策略规则来过滤恶意流量，并提供对网络访问的控制。防火墙可以根据预设的规则和策略来过滤不符合规定的流量，例如拦截来自未知来源或被认为是威胁的IP地址的数据包。通过限制不必要的流量进入网络，可以有效地阻止网络攻击和威胁。防火墙可以设置访问控制列表，以控制特定用户或主机对网络资源的访问权限。这样可以确保只有经过授权的用户或主机才能够访问受限资源，提高了网络的安全性。防火墙还可以实现网络地址转换，将内部私有网络IP地址与外部公共网络IP地址之间进行映射。这种转换可以隐藏内部网络的真实IP地址，增加了网络的安全性。防火墙可以记录网络流量和安全事件的日志，这些日志对于分析安全威胁、追踪攻击来源以及进行安全审计非常重要。通过对日志进行监控和分析，可以及时发现异常行为，并采取相应的措施来保护网络安全[4]。

2.2 入侵检测系统和入侵防御系统

入侵检测系统和入侵防御系统可以有效地监测和阻止恶意活动，提供对网络安全威胁的实时响应和保护。IDS是一种 passivesystem，通过监视网络流量来识别潜在的攻击行为。它使用预定义的规则和模式匹配技术，分析数据包和日志，以发现异常的活动。IDS可以检测到诸如端口扫描、恶意软件传播、未经授权的访问等网络攻击，并及时发出警报。它帮助了解当前网络流量中存在的潜在风险，从而有助于网络管理员采取进一步的安全措施。IPS则是一种 active system，不仅能够检测恶意活动还可以主动阻止这些攻击。与IDS不同，IPS具备拦截和响应能力，可以自动地对恶意流量进行过滤、屏蔽和阻止。当IDS检测到异常活动时，IPS会立即采取行动，以保护网络免受潜在风险的侵害。它可以根据事先设定的策略和规则，对入侵行为进行实时拦截和阻止，从而减轻攻击可能造成的损失。综合来说，IDS可以帮助及早发现潜在的安全威胁并发出警报，而IPS则能够主动地阻断恶意活动。它们的组合使用可以提高网络的安全性，保护个人、组织和企业的数据免受未经授权的访问和恶意攻击的侵害。然而，需要注意的是，IDS和IPS仅仅是整体网络安全策略中的一部分，还需要结合其他安全措施来建立一个完善的安全体系。

2.3 数据加密

数据加密采用特定的加密算法和密钥管理方法，将敏感信息转化为无法理解的形式，以确保数据在传输和存储过程中的机密性和完整性。数据加密的作用是防止未经授权的人员获得敏感信息，即使他们能够拦截或截获数据包。通过使用强大的加密算法，敏感数据被转换为密文，在传输过程中只有授权的接收方才能将其解密还原为明文，从而保护了数据的机密性[5]。另外，数据加密还可以保护数据的完整性，防止数据在传输过程中被篡改或损坏。通过对数据进行加密，可以附加校验和和数字签名等技术手段，确保数据在传输过程中不会被篡改，并且可以验证数据的完整性。在实际应用中，数据加密可以应用于多个层面，例如网络传输层、应用层、数据库层等。不同层面的数据加密技术具备不同的特点和适用范围，可以根据实际需求选择合适的加密方式。然而，要有效实施数据加密技术，还需要合理管理密

钥。密钥是解密数据的关键，必须妥善保管和更新，且只能授权给合适的人员使用。密钥管理需要考虑密钥生成、分发、存储和注销等环节，以确保密钥的安全性和可用性。

2.4 强密码策略

强密码策略要求用户在创建密码时使用复杂的组合，包括大小写字母、数字和特殊字符，并定期更换密码。这样做可以有效提高账户的安全性，降低密码被猜测或破解的风险。使用复杂的组合意味着密码应该由多个元素组成，包括大写字母、小写字母、数字和特殊字符。这样的密码具有较高的熵值（即不确定性），使得密码更难被猜测或通过暴力破解方式破解。例如，一个强密码可能类似于"7h#Gk2$D"，其中包含了各种类型的字符。此外，频繁更换密码可以减少密码被泄露后被滥用的机会。推荐的更换周期可以根据具体情况而定，通常建议每隔3-6个月更换一次密码。强密码策略能够增加攻击者破解密码的难度，降低被黑客入侵、数据泄露和身份盗窃等风险。然而，要确保强密码策略的有效性，用户也需要注意其他方面的安全措施，如不在公共场所输入密码、不使用易被猜测的个人信息作为密码等。

2.5 多因素身份验证

多因素身份验证要求用户在登录时提供多个不同类型的身份验证因素。传统的身份验证通常只要求用户提供用户名和密码，但随着网络攻击日益增多，这种简单的身份验证方式已经不再安全可靠。用户在登录时需要提供多个不同类型的信息，例如密码、指纹、短信验证码等。这些不同类型的身份验证因素结合起来，使得攻击者更难以冒充用户身份进行非法访问或操作。即使攻击者获取了用户的一个身份验证因素，例如用户名和密码，他们仍然无法成功登录，因为还需要其他的身份验证因素。例如，即使知道了正确的用户名和密码，攻击者没有用户的指纹或手机上的验证码，也无法通过身份验证过程。多因素身份验证可以大大降低账户被盗用和恶意访问的风险，提供更加安全的登录环境。同时，对于企业和组织而言，多因素身份验证也是一种有效的防范措施，可以保护公司的机密信息和重要资源。

2.6 安全更新和补丁管理

首先，操作系统厂商会持续监测并修复发现的漏洞，并将这些补丁发布给用户。通过及时安装这些安全更新，可以修复已知的漏洞，提升操作系统的安全性。同时，操作系统的更新还可以增加系统的稳定性和性能，提供更好的用户体验。其次，各种应用程序都可能存在漏洞，黑客可以通过利用这些漏洞来入侵系统。因此，应用程序的开发者会不断发布新的版本，修复已知的漏洞并改进功能。及时更新应用程序可以减少系统被攻击的风险，保护用户的隐私和数据安全。另外，路由器、交换机等网络设备也会存在安全漏洞，黑客可以通过攻击这些设备来入侵网络。网络设备厂商通常会发布安全补丁，修复已知的漏洞，并提供更强大的防御功能。及时更新网络设备的安全补丁可以增强网络的安全性，阻止潜在的攻击。

结语

总之，计算机网络安全技术的影响因素包括恶意软件攻击、网络钓鱼、拒绝服务攻击、数据泄露、身份欺骗和网络间谍活动。为了防范这些风险，可以采取防火墙、入侵检测系统、数据加密、强密码策略、多因素身份验证、安全更新和补丁管理、网络安全培训和教育以及安全审计和监测等防范措施。

参考文献

[1]熊鹰,赵红军.计算机网络安全技术的发展与趋势[J].计算机工程与设计,2021,42(3):1-6.

[2]高远,王琦,王洋.基于区块链的计算机网络安全技术研究综述[J].计算机科学,2020,47(10):1-7.

[3]周晓薇.计算机网络安全技术的影响因素与防范措施分析[J].现代电子技术,2020,43(03):175-177.

[4]张华,高志宇.计算机网络安全技术的影响因素与防范措施研究综述[J].计算机应用研究,2021,38(03):642-644.

[5]陈凯旋,李红艳.计算机网络安全技术的影响因素与防范措施研究进展[J].信息技术,2021,06:40-42.