基于应用视角的计算机网络安全技术完善分析

徐　彬

黄河勘测规划设计研究院有限公司云河科技　450003

摘　要：在现代化社会发展的背景下，计算机的应用已经相当普遍，为社会各个领域的进步奠定了坚实的基础。然而计算机网络在应用的过程中，往往都存在着安全问题，为了预防和控制这类安全问题，做好计算机网络安全技术的应用至关重要。因此，分析计算机网络安全问题，并基于应用视角提出计算机网络安全技术，对于维护计算机网络安全，推动计算机网络稳定运行，保障计算机网络健康可持续发展，具有重要意义。

关键词：应用视角；计算机网络；安全技术；完善

引言

为进一步强化计算机网络安全技术管理，需高度重视计算机网络安全技术的优化与运用，提高计算机网络系统的可靠性和安全性。

1 计算机互联网安全的重要性

在当今社会中，计算机网络已成为个人隐私泄露、商业机密泄漏以及国家安全威胁等问题的主要来源之一。因此，如何保证计算机网络的安全成为当前亟待解决的一个难题。一方面，计算机网络上的安全性问题是一个复杂的系统工程，涉及多个方面。从技术层面来说，计算机网络需要具备一定的防火墙、加密算法等防护措施来保护用户的数据和通信不受攻击者的侵害；同时，还需要建立完善的信息管理体系，加强对敏感信息的监管和控制，以确保其不被非法获取或者滥用；此外，对于一些重要的关键基础设施如电力、交通、金融等领域，还需采取更加严格的保障措施，以防止黑客攻击导致系统的瘫痪甚至崩溃；另一方面，计算机网络上的安全性问题的影响也非常深远。它直接影响个人的隐私权和社会秩序，一旦个人隐私泄露或者商业机密泄漏，将会给受害者带来巨大的损失和伤害；计算机网络上的安全性问题也会严重危害国家的安全利益，如果某个重要机构的机密信息遭到窃取或者破坏，可能引发严重的政治危机和社会动荡。计算机网络上的安全性是个十分严肃的问题，需要全社会的共同努力才能够得到有效的解决。

2 影响计算机网络信息安全的因素

2.1 病毒攻击

目前，网络上有着多种的病毒，而这些病毒对计算机系统的侵袭则是防不胜防。甚至有的病毒潜伏期长，隐藏性高，难以发现。虽然现阶段计算机系统之中安装了相应的杀毒软件，但并不意味着能够将所有的病毒都消灭。因为网络病毒有着传播速度快、危害大的特点，不容易被消灭，入侵计算机系统之后，必然会带来严重的危害，对计算机的使用产生影响。同时还会导致客户的信息被盗，甚至使得计算机系统出现瘫痪的情况，为个人或者企业带来严重的损失。

2.2 计算机系统漏洞与病毒

作为一种安全隐患，计算机系统漏洞可能被黑客用来进行攻击，这些漏洞可能由于软件设计或实现中的缺陷导致，黑客可用这些漏洞获取系统的敏感信息或者控制整个系统；同时，病毒常常依附于软件进行传播，并且其传播速度非常快。一项研究表明，全球每天有数百万个新的恶意软件样本被创建并分发，这些病毒可以通过电子邮件附件、可移动存储设备或者恶意网站等途径传播给其它计算机系统。一旦感染了病毒，计算机系统的性能可能会受到严重影响，导致系统崩溃或者变得缓慢；此外，病毒还可能破坏数据，导致用户丢失重要的文件或者信息。

3 基于应用视角的计算机网络安全技术完善措施

3.1 应用防火墙技术

在大数据时代下，信息安全成为用户最为关心的问题，并寻求相应的方法来避免计算机信息受到侵害。目前，对于计算机网络信息安全的强化上，防火墙技术作为传统的计算机网络安全技术，依旧发挥着良好的作用。对于防火墙技术的应用上，可以实现对计算机的网络环境进行安全防护，通过限制用户访问的方式，达到安全维护的目的。从防火墙系统来看，其是由软件和硬件所构成的系统。通常，在计算机操作系统之中应用防火墙技术，则可以对企图访问计算机的非法操作进行阻止，为计算机用户中的个人数据提供安全保障。另外，防火墙有着不同种类的技术，如转换型、代理型等，在使用的时候，用户需要依据不同的功能进行合理选择，以此来增强计算机的安全性。

3.2 及时进行系统漏洞的修补

及时修补系统漏洞是防范网络攻击的关键措施。尽管大部分系统漏洞都能够通过软件更新来修补，但仍然有一些漏洞无法得到完全解决。这主要是因为修补程序存在缺陷或者不完全适用于所有的系统环境，因此，制定高质量的修补程序至关重要。根据 NIST 的报告，修补程序应该经过充分的测试和验证，以确保其有效性和稳

定性；此外，修补程序的发布和部署也需要进行严格的控制和监测，以防止不当的操作或者未经授权的访问。只有确保修补程序的质量，才能有效地消除系统漏洞的安全隐患；最后，有效的系统漏洞修补需要依靠广泛的技术交流和知识共享，多国的研究成果和经验教训对于理解和解决系统漏洞问题具有重要意义，如 MITRE 公司的 CVE 数据库提供了全球最全面的系统漏洞信息和修补建议，可以帮助更好地了解和解决系统漏洞问题。

3.3 构建新型安全防护机制

随着网络攻击手段不断升级，传统的安全防护机制显得力不从心，迫切需要构建新型安全防护机制。这涉及采用人工智能（AI）和机器学习（ML）技术，通过深度分析庞大的网络数据，及时发现异常行为和潜在威胁，提高对未知攻击的识别能力。引入区块链技术可以加强身份验证和数据完整性的保护，构建去中心化的信任体系，使得网络安全更为可靠。这些新型安全防护机制的引入，使得网络安全策略更具前瞻性和适应性，为不断演进的网络威胁提供更有效的防范手段。建设网络人才团队。网络人才的培养是确保计算机网络安全的不可或缺的重要环节。为建设强大的网络人才团队，必须提供系统的安全培训和网络攻防演练等活动，培养出深谙网络安全领域的专业人才。鼓励人们从事网络安全研究，积极推动创新技术的发展，以不断提升网络安全水平。与此同时，积极与高校和研究机构合作，共同建立实践基地，为学生提供更多实际经验和机会。这种密切合作有助于搭建学术与实践的桥梁，培养出具备理论知识和实际操作经验的高素质网络安全专业人才，以更好地迎接不断演变的网络威胁和挑战。提高安全意识。人为因素是导致网络安全问题的重要原因之一。为预防社会工程学攻击等威胁，提高用户和员工的安全意识是至关重要的。通过定期组织网络安全培训，向用户传递关键的安全知识，让他们了解网络风险，并学会避免点击垃圾邮件、共享敏感信息等危险行为。举办网络安全宣传活动，以生动的方式向大众传达网络威胁的现实性和严重性，加深对网络安全的认知。共同形成的网络安全意识，使得每个用户都能够成为网络安全的守护者，积极配合组织的安全政策，共同维护网络生态的稳定和健康。

3.4 计算机网络身份认证技术

（1）用户名和密码：这是最常见的身份认证方式，在用户登录时需要输入正确的用户名和密码进行身份验证。但是，仅仅依靠用户名和密码存在被破解或伪造的风险，因此需要额外的认证手段来增加安全性。（2）双因素认证：双因素认证要求用户提供两项以上的验证要素，如密码、指纹、声纹、虹膜等。通过结合多个不同的验证要素，双因素认证极大增强了身份认证的安全性。（3）数字证书：数字证书是一种由可信第三方机构颁发的电子文件，用于证明在网络上的身份。它包含了身份信息和公钥等内容，可以用于身份验证和数据加密。（4）生物特征识别：生物特征识别技术利用个体独有的生物特征进行身份认证，如指纹、面部识别、虹膜识别等。生物特征是无法伪造的，因此具有较高的安全性。（5）单点登录：单点登录技术允许用户使用一个账号和密码登录到多个相关的系统中。这样可以减少用户需要记住的账号和密码，提高登录的方便性和效率。

3.5 数据加密

数据加密涵盖多个方面，包括数据传输、数据存储以及数据库加密，这些措施的目的在于保护敏感信息，确保数据的机密性、完整性和可用性。首先，数据加密在数据传输过程中发挥关键的作用。在信息传输中，数据可能会通过不安全的网络或通信渠道传送，这就使数据面临被黑客、窃听者或其他不法分子窃取的威胁。为了防止这些风险，通信协议如 SSL/TIS 等被广泛采用，以确保数据在传输过程中被加密。这意味着即使有人截获了数据包，也无法理解其中的内容，因为它们已被加密；其次，数据存储加密也是保护数据安全的重要手段。在大数据时代，数据通常存储在云端或大型数据中心，这使数据易成为攻击者的目标。数据存储加密是将数据在存储时加密，以确保即使存储介质被盗或访问，数据仍然安全。这为云存储、数据库和备份数据提供重要的安全性，从而减少数据泄露的风险。

3.6 完善网络信息安全方式

首先是完善网络基础设施建设，包括完善网络保障机制和网络信息安全技术。其次，提高企业和个人对网络安全的重视程度，强化网络安全防范意识和技能。除此之外，还应加强网络安全法律法规建设和执行力度。在网络基础设施方面，可以采取行业联动、政府引导等多种方式。例如，政府可以通过制定政策、出资建设网络基础设施、加强监管等方式，促进网络基础设施的发展。同时，可以通过行业协会的组织力量，推动网络安全、数据安全等方面的标准化建设，提升整个行业领域的信息安全水平。

结语

在大数据时代，计算机网络信息安全已成为一个不可忽视的问题。随着大规模数据的生成、传输和存储.网络攻击变得更加普遍和复杂。然而，随着技术的不断发展，也有更多工具和方法来应对这些挑战。保护计算机网络信息安全是每个个体和组织的责任，不仅关系个人隐私和财产安全，还关系社会和商业的持续发展。只有通过共同努力，才能确保在大数据时代中计算机网络信息安全得到充分的保护，以推动数字化社会的可持续发展和繁荣。

参考文献：

[1]陆卓遥.大数据背景下计算机网络安全问题与对策[J].网络安全技术与应用，2023（05）：62-63.

[2]陈登，张建敏.计算机网络安全中虚拟网络技术的运用分析[J].软件，2023，44（09）：22.

[3]郑春艳.云计算技术下的计算机网络安全探讨[J].现代计算机，2023，29（20）：73-75.

[4]刘城.大数据时代背景下计算机网络安全防范应用与运行[J].无线互联科技，2023，20（08）：166-168.