计算机网络工程的安全问题与解决对策

李 凯

广西壮族自治区信息安全测评中心 广西南宁

【摘要】信息技术的蓬勃发展对当代社会产生了巨大而深远的影响，一方面，便利了人们的工作与生活；另一方面，促进了整个世界范围内的信息资源的互通互享。然而，计算机网络工程的应用也带来了一些安全问题，明晰此类问题，并制定相应解决对策，能够有效提升计算机网络工程应用的稳定性与安全性，使之更好地服务于社会经济发展。

【关键词】计算机网络工程；安全问题；解决对策

Security Problems and Solutions of Computer Network Engineering

Kai Li

Guangxi Zhuang Autonomous Region Information Security Evaluation Center Nanning, Guangxi

【**Abstract**】The vigorous development of information technology has had a huge and far-reaching impact on contemporary society. On the one hand, it facilitates people's work and life; on the other hand, it promotes the exchange and sharing of information resources throughout the world. However, the application of computer network engineering also brings some security problems. Clarifying such problems and formulating corresponding solutions can effectively improve the stability and security of computer network engineering applications and make them better serve social and economic development.

【**Keywords**】Computer network engineering; Security problems; Solutions

新时期，计算机网络工程的应用深刻影响到了社会的方方面面，通过计算机网络进行资源的互通互联共享，极大地提升了人们的工作效率，同时也为人们的日常生活提供了巨大便利。然而，计算机网路工程的应用也不可避免地带来了一系列安全问题，基于共享基点的技术内核决定了不法分子能够利用相关技术或系统漏洞进行非法入侵行为，从而给计算机用户埋下安全隐患，严重时甚至会给用户带来较大经济损失，威胁到社会网络环境的和谐稳定发展。有基于此，应对现阶段计算机网络工程的安全问题予以深入剖析，在综合把握的基础之上探索针对性的解决方案，从而为计算机网络工程的安全稳定运行保驾护航。

1 现阶段计算机网络工程存在的安全威胁

1.1 系统漏洞

任何计算机系统在设计之初都无法实现绝对完备，加之不同用户的计算机使用领域不同，会导致计算机网路工程在实践应用中不可避免地遭遇系统漏洞威胁。这就要求相关管理人员定期对系统予以合适，及时排查潜在漏洞，进行补丁更新。

1.2 程序威胁

以木马、病毒等有害程序为代表的安全威胁类型亦是计算机网络工程应用过程必须正式的问题，随着社会经济发展日趋复杂化，通过计算机网络开展办公业已成为一种常态，病毒、木马等对计算机系统的攻击会致使网络瘫痪，进而影响到人们的正常工作生活。

1.3 身份识别威胁

身份识别环节出现安全威胁在计算机网络工程应用中较为常见，如受到随意口令、口令破解、口令圈套等问题的影响，计算机网路工程的安全性会受到削弱。以随意口令为例，部分用户设置用户名或密码时过于简单，对信息安全规范标准的符合程度不足，会让计算机系统处于易受到网络攻击的境

作者简介：李凯（1985-） 男，广西壮族自治区信息安全测评中心，工程师，研究方向：网络安全。

地。

1.4 物理威胁

计算机网络工程是一类硬件与软件相结合的综合性工程，在其运行过程中，网络硬件设备的安全性问题尤为重要，如设备遭遇偷窃，这一问题对于部分存储重要数据的网络设备而言尤甚，会让计算机网络工程应用所在单位产生较大的经济损失。

1.5 线缆连接威胁

计算机网络工程应用过程中，线缆连接环节也会产生相应的安全威胁，具体表现为冒名顶替、拨号进入、窃听等问题。如在线缆网络环境下，窃听问题干扰的影响较大；再如广播式网络系统内，由于在不同的节点均可获取相应网络信息，监视器安装、搭线窃听等问题的影响亦不容忽视。

2 当前计算机网络工程存在的主要安全问题

2.1 计算机网络工程安全意识不强

当前，仍然存在相当数量的计算机用户对信息技术的理解仅停留在应用层面，忽视了网络安全工作的重要性，意识层面的单薄导致计算机网络工程安全措施不够完善，开展安全防护的积极性不强，只有等到安全问题带来较大影响或较大损失时方引起重视。另外，计算机网络工程安全意识的缺失还会使得用户在进行操作时不能严格遵守相应规范标准，操作失当即会给黑客等不法分子的攻击行为创造有利条件。因而，现阶段普及计算机网络工程安全基础知识尤为关键，只有先从意识层面予以强化方能为后续安全防护技术的科学运用奠定基础。

2.2 计算机网络工程安全防护体系亟待完善

对目前计算机网络工程安全防护体系发展现状加以审视，可以看到，针对计算机系统的各项安全防护措施仍然存在不同程度的割裂性，即未形成多种安全防护技术以及措施的协同应用效果，导致部分计算机网络安全防护工作顾此失彼。如部分用户过于依赖防火墙技术，忽视了定期病毒查杀对计算机网络工程安全的保障，很多用户数月都未进行过一次安全检测，这无疑给计算机系统埋下了巨大的安全隐患。除此之外，成熟的计算机网络工程安全防护工作监督机制尚未建立起来，这一点在很多企业之中较为常见，制度的缺失往往导致对计算机网络工程安全防护工作的忽视。

2.3 计算机病毒

现阶段，计算机病毒无疑是影响计算机网络信息安全的主要因素之一，同其他威胁到信息安全的攻击行为不同，计算机病毒是人为编制的，且通过人们日常接触到的诸如邮件、新闻、软件等渠道进行传播，加之绝大部门计算机病毒具有自我复制的程序代码，其隐蔽性较强，能够在很短的时间内迅速感染大量计算机，破坏性较大。计算机一经感染计算机病毒，极易造成瘫痪的情况，更严重情形下还会在病毒的程序恶意操作下向其他用户的计算机进行病毒传播，威胁到计算机用户网络信息的安全获取及使用。步入新世纪以来，因计算机病毒引起的计算机网络信息安全事故时常见诸新闻端，给人们的工作与生活带来了不同程度的损失，这也在客观上促进了计算机网络信息安全技术的发展。

2.4 黑客攻击

黑客问题是现阶段计算机网络工程安全防护工作所关注的重点问题，新时期，世界范围内因黑客攻击造成企业或个人巨大损失的案例时有发生。黑客通常指的是部分具备较高计算机操作能力的个体或群体，能够通过系统漏洞实现巧妙侵入，对用户计算机系统中的数据信息进行窃取或篡改，以满足自身各方面的需求。当然，部分用户浏览一些具有伪装性的网站时，若安全意识不足也会给黑客窃取个人信息留下可乘之机，时下通过黑客攻击盗取用户信息进行非法谋利的问题日渐成为社会关注的重点。

2.5 不法入侵

网络犹如双刃剑，以信息高速共享巨大优势便利人们工作生活的同时，也不可避免地带来了一系列安全问题。目前，世界已然步入到大数据时代，人们对计算机网络工程的依赖性显著增强，网络信息的互联互通程度大大加深，但安全防护措施的不到位会给部分非法用户的入侵行为提供便利，其通过部分技术侵入到网络平台之中进行数据信息的窃取、篡改等行为近年来屡见不鲜，既影响到相关用户的信息安全，同时也会对数据信息传输的准确性与完整性产生负面作用。再者，更为严重的情况下，非法用户对计算机系统的入侵还能够直接篡改相应程序，导致计算机网络存在较大安全隐患，不仅软件无法正常运行，硬件也会受到损害，造成不同程度的经济损失。

3 计算机网络工程安全问题的解决对策探析

3.1 持续强化计算机网络工程安全意识

任何技术的应用最终都需要落实到人来实施，计算机信息处理技术亦然，故而，需要强化用户对计算机信息的安全防范意识。具体说来，应从以下几方面入手开展相关工作：一是不断规范用户的计算机使用习惯，可以制定相应的计算机操作使用标准，以此培养用户良好的操作习惯，从源头断绝因操作不当导致的计算机信息安全隐患；二是杜绝盗版软件的使用，坚持从正规渠道（如官方渠道）购买所需要的计算机软件，防止因盗版软件漏洞导致的信息泄露情况发生；三是加强计算机信息处理安全意识的宣传教育，让防范意识根植进用户脑中。

3.2 建立科学健全的计算机网络安全防护体系

健全的计算机网络安全防护体系之中，防火墙系统是应用最为广泛且安全防护效果较为有效的方式之一，对于未取得授权的非法用户访问行为，防火墙系统能够予以有效拦截，从而防范其对计算机系统的侵入乃至破坏。作为一类基于信息传递过程的安全防护技术，防火墙可以在读取网络信息时较为准确地判断网络信息的安全性，并采取自动拦截措施。此外，运用防火墙技术的同时增设双网关运用，可应对很多黑客与病毒隐蔽性入侵行为，从而对防火墙安全防护效果予以进一步强化，并切实提升网络信息传输效率。

3.3 定期开展病毒查杀与漏洞修复工作

计算机网络工程受到蓬勃发展的信息技术影响，其应用广度与应用深度均实现了巨大拓展，与此同时，也带来了各种类型的安全问题，其中，尤以计算机病毒问题为甚，现阶段的计算机病毒发展呈现出多样化与复杂化的趋势，且隐蔽性显著增强，对于部分计算机网络安全意识不强的用户而言，极易受到此类文件的欺骗，使之侵入到系统之中。为此，需要定期开展病毒查杀工作，结合用户自身计算机实际情况选择针对性的杀毒软件，同时选取符合具体情形的杀毒方式，如快速杀毒、全面杀毒抑或是指定区域杀毒等。再者，还需要定期修复计算机系统漏洞，目前计算机系统之中微软公司的产品占绝大多数，虽然会定期予以更新对部分漏洞进行修复，但为进一步提升计算机系统安全性，还需要定期使用相关专业软件对其他潜在系统漏洞进行排查修复，让计算机网络工程运行更为安全可靠。

3.4 综合运用数据加密技术

开展计算机网络工程的安全防护工作，必须对数据加密技术的重要作用予以充分正视，缘其能够大大降低网络信息于传输过程可能存在的泄露风险。综合运用好数据加密技术，具体可通过对应密钥或算法来实现计算机网络中信息向隐秘性数据的转变，而唯有正确使用密钥方可获取此类数据。与此同时，为进一步强化数据加密效果，还可以使用信息解密手段，这样可以有效提升整个信息传输过程中的可靠性与安全性，但需要相关人员能够对信息加密方式予以透彻了解，在此基础上对用户身份进行核准，并在发现用户利用信息进行不法行为时及时对账号予以封禁处理。此外，还应根据用户实际情况选择符合自身的加密技术类型，一般而言，链路数据加密技术、节点数据加密技术以及端端加密技术在计算机网络工程运行时较为常见，因而需根据具体情况予以科学选择。

3.5 科学配置入侵检测系统

对于计算机网络工程易受到黑客及不法分子入侵的问题，应通过入侵检测系统的科学配置加以应对，以此实现对网络数据的动态辨别与分析，从而及时排查入侵行为，保障计算机网络工程运行安全。具体而言，应从下述几个方面入手开展相关安全防护工作：（1）科学运用身份认证系统，与此同时实现该系统与防火墙的协同应用，从而立足于全过程视角对计算机网络上的各类型活动予以细致检测，通过反复确认防火墙以外用户身份，具体可采取二代居民身份证、指纹比对、人脸识别等方式，对进入到系统中的用户进行从严把控；（2）采取具有针对性的访问权限限制方式，对相关用户的访问权限予以严格管控，通过对访问用户权限的科学认证，能够最大限度地保障计算机网络工程的安全性与稳定性，进而让计算机网络中的关键资源避免受到不法浏览或使用。

3.6 秉持细致化原则做好数据备份工作

数据备份是计算机网络安全防护中的一道稳固防线，自然灾害、物理损坏、系统崩溃、操作失当等问题发生后，依托细致而完整的数据备份成果，不论是企业或个人均能迅速回复到正常的生产生活之中，从而将上述影响所造成的经济损失降到最低。通常而言，可根据用户实际情况选择完整备份、差异备份、递增备份等方式，总而言之，数据备份工作是对前述计算机网络工程安全防护措施的有效补充，数据备份技术的科学运用以及备份过程的细致

化能够给予计算机系统文件一份高度安全保障，进而有效避免因病毒侵入、黑客入侵等造成的损失扩大化。

4 结语

计算机网路工程在实际应用过程中需对安全问题予以充分重视，一方面，应从计算机网络工程安全意识层面入手开展相关工作，通过持续强化宣传教育，提升人们的计算机使用规范性；另一方面，应选择科学的计算机网络安全防护举措，协同应用好多种计算机网络工程安全防护技术，从而构筑起健全的安全防护体系。此外，还应坚持细致化原则，做好计算机系统的数据备份工作，为安全防护筑牢最后一道防线，为计算机网络工程的可靠稳定运行奠定起坚实的基础。

参考文献

[1] 黄涵石. 计算机网络工程安全问题及其对策探讨[J]. 信息通信, 2015(10):2.

[2] 于澎灏. 计算机网络工程安全问题及其对策[J]. 数码世界, 2017(10):1.

[3] 张媛. 计算机网络工程安全问题及其对策[J]. 工业, 2016, 000(007):P.70-70,134.

[4] 阎宁, 王策源. 计算机网络工程安全问题与解决策略探析[J]. 城市建设理论研究:电子版, 2016, 000(009):1217-1217.

[5] 张文婷. 计算机网络工程安全问题与解决策略探析[J]. 新商务周刊, 2016, 000(005):75.

收稿日期：2022 年 3 月 9 日
出刊日期：2022 年 5 月 12 日
引用本文：李凯，计算机网络工程的安全问题与解决对策[J]. 工程学研究，2022，1(1): 35-38
DOI: 10.12208/j.jer.20220009
检索信息：中国知网（CNKI Scholar）、万方数据（WANFANG DATA）、Google Scholar 等数据库收录期刊