网络信息安全技术管理的计算机应用探讨

李金荣

中国电信股份有限公司银川分公司

摘　要：随着信息时代的降临，人们信息获取的途径基本是互联网，网络信息传递已经成为当前人类社会生活不可或缺的一部分。因此，信息安全就成了需要进行深入研究的一个方向，如何利用有效的网络技术以及计算机技术进行网络信息安全管理等也是研究的一个重点。如今在网络信息安全中所包含的，又从更多的方面进行了内容更新，包括信息传递的安全性、信息在遭受网络攻击时候的安全保障、计算机系统和网络系统的信息安全防范、系统内部的信息安全检测、系统的信息安全控制、网络信息安全技术管理的管理制度设计、网络信息传递的安全风险评估等。网络信息安全的建立，依赖复杂的网络以及计算机技术本身，而这些技术的掌握群体具有复杂性，它包含各类的计算机人员、互联网行业从业人员等，顶尖技术的掌握人群也是复杂的，其中不乏会造成犯罪的不法分子，这些危险因素都会对网络信息安全造成破坏。另一种就是外界因素，在进行网络信息安全维护和技术管理的时候，计算机技术的应用一般形式为安全防护屏障的打造，其中防火墙等技术就是比较常见的安全维护手段。

关键词：网络信息；安全技术；计算机；应用；分析

【DOI】10.12252/j.issn.2096-6288.2023.11.228

引言

随着技术发展的逐渐深入，网络信息安全所包含的内容也在不断地发展和扩张，从最开始仅仅从安全性出发的信息安全性定义以及信息保密性定义；到后来对信息的完整性、对网络信息的可用性、对网络传递的信息是否具有充足的可控性以及对信息是否能够否认也做了要求，这一时间段，网络信息安全开始跟着技术和社会需求的发展进行第一次的含义扩充；在信息时代，计算机网络已成为社会生活和商业运营的重要基础设施。然而，随着网络规模的扩大和数据量的急剧增加，网络安全问题也变得愈发严峻。大数据技术的快速发展为网络攻击者提供了更多的机会和工具，以便发动复杂、难以防范的网络攻击。因此，迫切需要研究和实施适应大数据背景下的网络安全防范策略，以保护网络的完整性、可用性和机密性。当前网络信息传递的载体就是各种类型的网站以及计算机应用软件等，在计算机管理和应用中，对于网络信息安全技术的管理成为信息时代的热门项目。为了能够保障网络信息安全进行良好的技术应用，需要结合计算机特性以及网络信息时代的优势，切实地对计算机的网络信息安全进行强化，进而促进信息技术的发展。

一、分析计算机网络安全的特点

（一）分析动态性的特点

计算机网络的动态性体现在网络环境的不断变化，网络拓扑和流量以及用户行为、应用程序都是在持续的演化，新的硬件设备、软件更新、用户连接和应用程序部署不断涌现，这为网络威胁提供了机会。网络安全仅是一次性防御措施，而必须是一个持续的过程，能够及时适应新的威胁和漏洞。

（二）分析全面性

网络安全是一个多维度问题，需要全面覆盖各个网络层面和相关领域，在不同网络层面包括物理层、数据链路层、网络层和传输层等等，都存在着各自的威胁和安全挑战，例如物理层面可能涉及硬件设备的物理保护，而应用层面可能涉及应用程序漏洞的防护。此外，还要考虑硬件和软件的安全性，以及人员、政策和法律等多个方面的安全问题。

（三）分析复杂性

网络安全的复杂性体现在多个技术和概念的相互作用，安全技术包括了加密和身份验证以及访问控制、防火墙、安全策略等等。这些技术需要在复杂的网络环境中协同工作，以提供全面的防护。例如，入侵检测系统能够检测到潜在的攻击，但防火墙需要阻止这些攻击进入网络。安全策略要考虑如何平衡安全性和便利性，以满足用户和组织的需求。网络安全还要不断适应新的威胁和攻击技术，这增加了复杂性。

二、现阶段计算机网络信息安全问题分析

（一）计算机网络存在的脆弱性

根据计算机网络信息安全现状可知，由于计算机网络自身具备的开放性以及包容性等充分的为信息传递、文化交流等提供了比较方便、高效的平台，但是其数据共享性也进一步为数据信息的传递创造出良好的环境，

这些在一定程度上都是计算机网络的优点。但从另一方面分析可知，网络信息存在的环境不仅是复杂的，同时也是多变的，其中会对网络自身的安全性以及复杂性进行涉及。计算机应用的可靠性、稳定性等，多种条件的叠加导致信息的安全问题保障成为一项艰巨的工作。其中最突出的就是计算机网络，计算机网络的开放性不仅会带来方便，同时带来的还有许多的网络安全问题，强开放性网络遭受攻击的风险就比较高，这对于网络信息的安全来说带来的威胁就更高了。另外，计算机网络的国家性会导致网络攻击的范围变得比较广，这种威胁从国家上分析，国际网络犯罪就是通过互联网进行的，这些安全问题不仅威胁着人们的个人信息安全，甚至还会威胁国家机械信息安全等。

（二）计算机网络防火墙比较脆弱

计算机技术问题中比较主要的信息安全维护就是防火墙技术，结合网络信息，其防火墙是对安全给予维护的重要保障策略。对于防火墙而言，其应用范围主要分为内部网络和外部网络这两者之间的交流、专用网络以及公用网络之间，这对于用户本身的信息安全起到了一定的保障。在计算机中，通过合理的运用防火墙，能够对用户的网络信息安全给予保护，通常状况下，在连接某个网络的过程中，计算机会对用户进行信息接入询问，以确保用户是否同意同一网络下的其他设备发现本设备，这也是对用户信息的一种保护。结合当前可知，防火墙技术也会随着网络技术的快速发展而进行发展，这对我国的网络安全保障来说属于一大助力，但由于防火墙不能对所有类型的攻击进行主动抵抗，再加上科技的不断发展导致攻击手段变得极具复杂，所以防火墙的安全性也进一步遭受了比以往更大的威胁。

（三）分析网络安全意识问题

在现如今时代背景下，虽然沉浸在数字世界中，但是网络安全意识相对比较薄弱，这一个问题主要表现在很多层面上，许多普通用户对网络安全问题的重要性不够重视。他们可能不会采取足够的措施来保护自己的在线隐私和数据，从而容易成为网络犯罪分子的目标。此外，企业和组织中的员工也可能缺乏必要的网络安全教育，导致他们在工作中不慎泄漏敏感信息或容易受到社交工程攻击。尽管网络安全威胁日益严重，但仍然存在许多组织和企业的网络安全管理不够到位的问题。这包括不及时更新和维护网络设备、不充分的风险评估、缺乏全面的安全策略和流程等。这些问题导致了网络漏洞的存在和威胁的不断滋生。

（四）分析计算机系统问题

在现如今时代背景，计算机系统面临着日益复杂的软硬件条件，其中存在很多的漏洞问题，这些漏洞问题可能是因为程序的错误和不安全配置以及过时软件或者是第三方组件的脆弱性引起的。黑客和攻击者往往利用这些漏洞来入侵系统、窃取数据或发起恶意攻击。即使一些漏洞已被识别和修复，但由于许多系统不及时升级或修补，它们仍然存在，并构成潜在的风险。在此之外木马病毒的传播问题。木马病毒是一种恶意软件，它通过伪装成合法程序或文件，悄无声息地侵入计算机系统，然后在背后执行各种恶意活动。在大数据时代，木马病毒的传播变得更加隐蔽和普遍。它们可能附加在下载的文件中、伪装成常见的应用程序，或者通过社交工程手段欺骗用户进行安装。一旦成功安装，木马病毒可以窃取个人信息、监视用户活动，甚至成为大规模网络攻击的一部分。

（五）分析黑客恶意攻击

在现如今的时代背景下，网络黑客依然是网络安全的重要威胁，可能是个人恶意黑客以及犯罪组织或国家级黑客团队，这些黑客是应用各种高级的工具和技术，例如高级持续性威胁（APT）、分布式拒绝服务（DDoS）攻击和零日漏洞利用，来渗透网络、窃取数据、破坏基础设施或进行间谍活动。这种形式的恶意攻击通常需要高超的技能和资源，给网络安全带来了巨大的挑战。

三、分析网络信息安全的计算机应用以及其发展策略

（一）分析身份验证技术

网络信息安全的维护工作，是依赖于各种技术的支持，在各大应用软件和网站之中，较为常用的安全保障技术之一就是身份验证技术，在对信息进行传输的过程中，身份验证技术能够更好的对用户的身份进行确认，通过确认的用户才可以进行信息获取和传递等工作。身份验证技术包含用户信息确认以及活体确认，在确保信息正确的情况下，还要对参与确认的用户是否是真实存在的而非网络攻击创造的虚拟用户。信息确认包含对用户个人注册信息的确认以及对用户权限信息的确认，通过全新的限制来管理用户可以访问的信息类型，这也是

避免信息泄漏的一个有效手段。

（二）分析防火墙技术

防火墙是信息安全管理的一个重要防线，也是最为基础的一个防线，在计算机运行的过程中，有效的防火墙设置是可以对外界的不法访问进行拦截，针对未经过授权的用户访问时，防火墙就相当于一道屏障，将这些非法访问进行隔离，进而确保本机网络信息传输的安全。防火墙从一开始的过滤型防火墙发展到现在的复合型防火墙，也是针对时代网络特性进行的改变，面对木马攻击以及IP欺诈等手段时，防火墙可以通过多种防护措施的结合来进行防护，同时，还可以在多种层面进行安全防护，例如，在信息传输层面的防护、在网络层面的防护以及在计算机应用运行层面的防护等。

（三）分析入侵检测技术

在网络信息安全技术管理的过程中，各种类型的技术应用是层出不穷的，其中入侵检测技术便是一项针对信息泄漏和丢失等问题所应用的安全管理技术，这个技术的应用主要是分为了三个阶段，对用户的信息以及应用信息进行收集、将收集的信息进行归纳和分析、对数据信息分析结果进行相应的处理。也就是在应用运行期间，对用户行为产生的日志信息、系统信息、用户信息等等进行采集，并确保信息足够全面，然后对信息进行分析和整理，根据信息的痕迹来判断该应用是否存在网络入侵的行为，根据判断的结果进行相应的处理。

（四）分析病毒防护技术

病毒是作为威胁网络信息安全的重要源头之一，通过有效的病毒防护技术可以对计算机的病毒问题进行防治，不仅仅可以提高网络信息安全管理能力，也是可以保证计算机在运行的时候，正常的功能不会因为病毒而影响和破坏。现如今我国的病毒防护类型比较多，用户在进行病毒防护措施选取的时候，可以结合具体的应用需求进行选择。目前，普通的计算机用户使用的最广泛的病毒防护技术就是下载病毒防护软件，通过软件定时的病毒检测来计算机中的病毒进行发现和清除；同时，防病毒软件也实时地监测着计算机的情况，当计算机出现病毒入侵时，就会在第一时间向用户发起警告，例如，在用户安装某一个应用的时候，防病毒软件对其检测后发现其携带了病毒，这时就会警示用户不要进行安装。这种快速探查病毒的方式，能够让用户及时地对计算机中的病毒进行发现和控制，使其可以更好的去保证计算机的应用安全，保证其网络信息的安全性。

总结

总而言之，在网络信息发展以及计算机快速发展的时代，网络成为人们进行交流的主要媒介，这些时代的科技产物也反向地作用于时代，进而改变了人们的社会生活方式。未来的研究方向包括进一步改进网络安全算法和技术，提高网络安全策略的自动化程度，以及加强国际合作来共同应对全球性的网络安全挑战。通过不断创新和改进，能够更好地保护计算机网络，确保其在大数据时代发挥其最大潜力。网络技术带来了生活的便利，同时也带来了一定的风险，最近几年，最严重的问题就是网络信息安全问题，如果不能对这些问题进行有效的处理，那么网络带给人们的优势就会随着问题的加重而消失。这时，就需要社会各界针对这些问题提出相应的解决策略，进而通过政策、技术等来维护网络信息的安全。

参考文献

[1]崔纪飞.信息加密技术在网络安全中的应用研究[J].西藏科技，2023，45（10）：69-76.

[2]顾丽旺；梁娜；初晓翠；徐风；张运涛；王曙光.基于区块链技术的互联网信息安全思路探索[J].网络安全技术与应用，2023，（10）：16-18.

[3]吴凌云.数据加密技术在计算机网络安全中的运用分析[J].信息记录材料，2023，24（09）：44-46.

[4]闫军.数据加密技术在计算机网络信息安全中的应用研究[J].信息记录材料，2023，24（09）：152-154.

[5]孙悦.人工智能技术在计算机网络发展中的应用探讨[J].中国新通信，2023，25（16）：78-80.

[6]魏晓微.基于大数据的计算机网络信息安全与防护策略[J].电子技术，2023，52（08）：49-51.

[7]邓诗钊.计算机网络信息安全中虚拟专用网络技术的应用[J].信息系统工程，2023，（08）：84-87.

[8]高航；于航；王利舟.关于信息安全与信息技术国产化的思考分析[J].网络安全技术与应用，2023，（08）：160-162.

[9]韩珺；杨莉莉.计算机通信网络的安全防护策略分析[J].集成电路应用，2023，40（08）：186-187.

[10]刘永辉.计算机网络信息安全中虚拟专用网络技术的运用[J].科技资讯，2023，21（15）：20-23.