计算机网络安全面临的威胁及其防范措施

王 麟
(哈尔滨市产品质量监督检验院,黑龙江 哈尔滨 150000)

摘 要:在我国社会和经济不断发展过程中,由于人们的生活和工作方式不断转变,为计算机网络技术应用提供更多的发展空间,并为信息和数据传输营造良好的环境。因此在目前城市建设发展过程中,需要相关部门增加计算机网络系统建立,并制定严格的管理制度,从而确保信息数据能够为人们的生活和工作提供便利条件。作为计算机网络技术应用核心基础,需要技术人员根据实际网络运行情况,同时按照计算机网络技术发展方向,能够为计算机网络构件安全稳定的运行环境,并能够为我国相关行业基础设施建设提供丰富的应用条件。本文围绕计算机网络安全问题展开讨论,目的是能够制定相应的管理措施,从而对计算机网络中出现的威胁起到有效的防范作用,并为相关防护措施制定提供参考价值。

关键词:计算机;网络安全;防范措施
中图分类号:TP393 文献标识码:A 文章编号:2096-4390(2019)14-0087-02

在现代社会发展过程中,由于计算机网络技术普及程度不断升高,并作为人们生活和工作重要的组成部分,能够为人们提供更加便利使用条件。因此在目前计算机网络建设过程中,十分重视人们使用体验,并根据数据信息传输时效性和安全性进行充分的研究,目的是确保传输的信息能够在安全的环境中产生良好的价值。但是针对不断出现的计算机网络安全问题,成为我国相关政府重点关注对象,由于计算机网络安全问题会给人们在使用过程中产生巨大的影响,从而降低人们对计算机网络技术的使用,导致许多行业发展受到不同程度的制约。所以在今后计算机网络技术应用过程中,需要相关部门加大安全防护研究力度,增加多种有效措施使计算机网络受到良好的保护,进而降低由于网络安全引发的社会负面效应。

1 计算机网络安全事件

在目前计算机网络系统建设和运行过程中,由于人为或者多种因素的影响,导致计算机网络受到不同程度的破坏,并最终出现计算机网络安全事件,不但使人们生活和工作受到严重的影响,同时也为社会发展造成不同程度的负面效应。因此为提升计算机网络安全,需要根据计算机网络具有的特点,能够针对具体问题展开相关研究和分析,从而为制定相应的网络安全保护措施提供良好的基础。在进行计算机网络系统建设过程中,网络硬件设备和软件设备作为组成基础,因此在保护计算机网络系统过程中,需要针对上述两方面增加相应的保护措施,进而确保计算机网络系统安全稳定的运行。在人们使用计算机网络系统过程中,产生的数据和信息需要进行及时的传输,并根据产生的价值实施报货措施,从而防止不法分子对书籍信息进行偷取,能够为个人或者企业的经济效益起到积极的保护作用。

2 计算机网络安全威胁分类

2.1 基本威胁。为提升计算机网络系统在使用时产生的价值,需要按照信息数据具有的以下作用制定保护措施:⑴ 机密性;⑵ 完整性;⑶ 可用性;⑷ 合法使用。因此围绕上述信息基本使用原则,需要在进行计算机网络安全防护制定过程中,能够针对以下四点威胁因素进行研究:2.1.1 信息泄露。通过计算机网络进行信息传输,能够在多个用户间建立传输通道,从而确保信息能够及时准确的到达。但是由于信息传输过程中会出现泄露情况,并通过以下方式对信息进行破坏:⑴ 窃听;⑵ 搭线;⑶ 盗取;⑷ 篡改。2.1.2 完整性破坏。根据数据传输要求和标准,要完善数据保护机制,从而减少由于多种因素导致数据完整性遭到破坏。2.1.3 拒绝服务。通过计算机网络系统能够实现多个用户进行交流,并在每个用户间提供相应的网络服务,从而确保数据信息能够得到正确的传递,但是在实际传输过程中,会由于用户网络无法承担信息应用要求,从而造成用户进行交流产生的服务无法正常进行。因此在用户使用计算机网络系统过程中,由于出现拒绝服务现象,从而造成更多信息数据交流出现障碍,并最终出现恶性循环的状态。2.1.4 非法使用。用户通过计算机网络将信息进行传输过程中,由于信息具有时效性和真实性,需要对用户对产生的信息进行分辨,从而确保获得信息的使用权。但是通过计算机网络对信息进行篡改或者盗取,能够转变信息的使用权,进而造成信息发生非法使用现象。根据信息出现非法使用可以判断,在进行网络安全保护过程中,需要针对信息出现非法使用情况进行综合性分析,进而制定有效的应对措施。

2.2 主要的可实现威胁。在上述计算机网络安全威胁中,由于实际网络运行条件和情况会出现多种变化,从而能够为主要的可实现威胁产生积极的作用。因此在实际网络安全维护过程中,需要将潜在的风险因素进行预防,并能够将可能实现的威胁作为优先处理目标,从而降低可实现威胁对计算机网络产生的安全问题。在目前出现的主要可实现威胁中,需要按照以下出现的威胁进行研究和分析:2.2.1 假冒。在多个用户进行信息数据传输过程中,由于网络中具有潜在假冒信息的风险,通常能够进行伪装,从而潜入到网络中,并对安全防护措施产生致命的影响。作为网络安全重要的防护方式,需要对信息进行具有的真实性进行审核,从而降低由于信息假冒导致网络安全问题不断出现。2.2.2 旁路控制。在计算机网络运行过程中,需要将特殊性质的信息和数据建立安全防护体系,并增加防护体系抗干扰能力,从而降低由于不法分子对网络进行攻击,导致网络出现多种安全问题。因此在网络建设过程中,需要增加对旁路设备的控制监督,进而对风险因素进行有效的防控,使网络环境更加安全稳定。

2.3 授权侵犯。根据信息数据具有的价值,在不同用户进行传输过程中,需要按照信息的特性进行授权管理,并对每个用户明确信息的授权范围,从而有效减少信息出现的授权侵犯问题。在目前信息出现授权问题中,主要由以下威胁问题存在:2.3.1 特洛伊木马。在目前计算机网络安全威胁中,根据破坏性和产生的影响范围,将特洛伊木马病毒作为重点研究对象。由于在计算机网络中运行程序受到特洛伊木马病毒影响,从而能够将病毒程序植入到程序中,使计算机网络出现不同的 (转下页)

六自由度磨骨机器人磨头装夹设计

雷春翠
(哈尔滨瑞博特机器人技术有限公司,黑龙江 哈尔滨 150000)

摘 要:近些年来,随着电脑的频繁使用和智能手机的出现,颈椎病频发,颈椎间盘置换手术越来越多,然而传统的人工颈椎间盘置换手术有许多问题,例如手术精度不足、手术辐射过多、医生工作强度大等等问题。六自由度磨骨并联机器人的产生解决了这一问题,不仅提高了手术精度,减少了辐射,还减轻了医生的工作强度。在六自由度磨骨并联机器人中有一关键结构,那就是磨头部分。由于其磨头部分与人体直接接触,因此磨头的安装牢固就显得极为其重要,为避免磨头装夹部分不牢固影响手术以及方便更换不同型号磨头,特进行磨头装夹部分设计。本设计提出了六自由度磨骨机器人磨头装夹设计部分的各部分名称、结构原理、结构要点及设计结论。

关键词:六自由度 磨骨 机器人 磨头 装夹
中图分类号:TH789 文献标识码:A 文章编号:2096-4390(2019)14-0088-02

1 六自由度磨骨机器人磨头装夹设计要求

1.1 设计时充分考虑装夹后的磨头刚度

在本次装夹设计当中,六自由度磨骨机器人的磨头采用标准器件截取而成,磨头部分是直径只有 4mm 粗的球体,磨杆则是直径只有 2.35mm 粗的杆状体,长度却达到 47mm 长,属于细长杆类型,刚度较差,因此在装夹设计时一定要充分考虑到装配后的刚度问题。使得在进行磨骨操作时不产生大变形。因此装夹部分结构应该不可过长,以免影响磨头装夹后的刚度。

1.2 装夹结构尺寸应该尽量减小

因手术固有空间是固定的,所以磨头装夹结构应该越小越好,这样可以增加六自由度磨骨机器人的工作角度,提高手术效果。因此在设计时一定要在保证质量的同时在宽度方向上尽量减小。

1.3 装夹结构应该便于拆卸

磨骨机器人在工作过程中需要更换不同类型的磨头,为了减少病人的手术时间,提高手术效果,磨头装夹结构应该便于拆卸,减少手术的无效时间,减轻病人的痛苦和医生的劳动强度。

1.4 装夹结构必须牢固可靠

由于磨头是进入人体手术的器械,因此它的装夹结构必须牢固可靠,否则就会引起严重后果,造成医疗事故,因此磨头装夹结构必须保证牢固可靠。

1.5 装夹结构需经久耐用

(转下页)

问题。另外如果用户将病毒程序进行阅读或者传递,致使影响范围不断扩大。2.3.2 陷门。按照计算机网络运行特点,在对不同程序和文件进行阅读过程中,由于进行相应的管理,需要对特定的内容下达指定命令,致使计算机网络设备出现陷门状态,进而导致更多的错误指令出现,致使计算机系统出现安全问题。

2.4 潜在威胁。围绕计算机网络技术应用特点,在网络中出现安全潜在威胁中,需要根据产生的影响制定相应的解决措施,并防止潜在威胁扩大影响范围。在目前计算机网络潜在威胁中,主要出现以下几种情况:⑴ 窃听;⑵ 业务流分析;⑶ 人员疏忽;⑷ 媒体清理。

3 网络安全管理及防范措施

3.1 应用加密技术和数字签名。随着计算机安全防护系统不断建立,在目前计算机网络增加相应的保护措施,并将加密技术和数字签名作为控制方式,从而能够有效提升计算机网络安全管理效应。另外在许多特殊计算机网络环境中,通常将 S/MIME、PGP、GPG 等加密工具作为防护措施,从而提升数据信息传输保密性和安全性。

3.2 VLAN(虚拟局域网)技术。在目前常用计算机网络保护措施中,将 VLAN 技术作为信息链路层保护方式,并能够在用户进行信息传输过程中,实现多种设备和网络环境内产生良好的保护作用。根据 VLAN 技术建立的虚拟局域网络,能够实现信息数据具有稳定的抗干扰能力,同时防止不法分子对网络进行攻击。

3.3 防火墙技术。在计算机网络技术应用过程中,由于多个用户对于信息数据的要求不同,从而为计算机网络应用防护墙技术,并在规定时间内完成对系统的检测和防护,进而提升网络安全管理和控制能力。作为目前常用防火墙技术应用过程中,需要根据网络风险因素进行优化和调整,从而使计算机网络防火墙具有的作用不断提升。

3.4 杀毒软件。随着计算机网络风险因素不断增加,技术人员根据网络病毒的变化,研制相应的杀毒软件,并在计算机网络内进行安装调试,从而在网络关键位置建立防护体系,为用户电脑产生良好的保护作用。

3.5 灾难处理与数据备份。在计算机网络运行过程中,一旦遇到特殊情况发生,并对计算机网络产生毁灭性破坏,从而使计算机网络内的数据信息出现丢失或者隐藏。因此在出现特殊问题情况时,需要计算机系统能够具有良好的灾难处理能力,并将相应的数据信息进行备份,从而确保用户或者企业的经济利益不受损失。

结束语

综上所述,在我国目前计算机网络技术应用范围不断扩大过程中,需要根据网络风险潜在因素的产生,制定相应的预防措施,同时按照计算机网络发展趋势,不仅要为人们生活和工作提供更加便利的条件,同时也为计算机网络发展奠定坚实的基础。

参考文献

[1]郭正红,胡世锋.常见网络攻击手段及安全策略[J].电脑知识与技术,2008,(5) 52.
[2]谭瑛.计算机网络的安全威胁及其防御机制研究[J].电脑知识与技术,2009,(24):122.
[3]汪海慧.浅议网络安全问题及防范对策[J].信息技术,2007(1) 40.