计算机通信网络安全隐患及其对策探讨

常素丽

（河北政法职业学院　河北　石家庄　050600）

[摘　要]计算机是现代人工作和生活中至关重要的组成部分，人们在享受计算机网络所带来的便利条件的同时也需要承担起通信网络安全风险，要正视其中存在的各种安全隐患问题。本文将就计算机通信网络安全隐患及其对策的相关内容进行深入分析和探究。

[关键词]计算机；通信网络；安全隐患；对策

【DOI】10.12252/j.issn.2096-6261.2021.12.1553

在网络通信全面发展的背景下，现代人与网络之间的联系越发紧密。当前，为了保证计算机网络价值的充分发挥和体现，让人们享受到更好的计算机体验感受，其必须要高度重视起计算机通信网络安全问题，及时寻找到其中存在的网络安全隐患，并制定出更具针对性的解决对策。

一、关于计算机通信网络安全的介绍

目前，计算机通信网络共包含两项核心技术，其一是计算机具体技术，其二便是通信网络具体技术。由此可以看出计算机通信网络安全主要会涉及到两个方面的安全内容，其一是计算机具体技术安全，其二是通信网络技术的安全。计算机网络通信，以计算机为载体和媒体来实现网络通信的目标，通过综合处理和存储收集到的信息数据内容，来进一步保证计算机网络通信的理想效果。在全新的社会发展形势之下，现在计算机网络已经成为现代人工作和生活中不可或缺的重要内容，计算机网络通信的安全更是直接关乎着亿万网民获取信息的质量和感受。所以，计算机网络通信安全一直都是相关领域工作者重点关注的内容。当前，计算机网络技术发展势头越发强劲，现代人对计算机网络技术的依赖性也越来越强，不管是个体还是单位，其信息和紧密都包含在其中，其必须要进一步加强对计算机通信网络安全的重视。此外，计算机网络技术人员还需要下意识去创新和完善相关工作内容，要尽全力去确保计算机用户的信息安全，同时要帮助广大用户获得更好网络使用体验和感受。

二、计算机通信网络安全的重要性

计算机通信网络初期，是在1969年，雏形是阿帕网，阿帕网的组成只有4台电脑。而现如今的计算机网络已经实现了质的飞跃，其不仅将区域、国家联系到了一起，而且连接范围已经拓展至整个世界，因为有了计算机网络的出现和应用，现代人的生活联系越发紧密。近些年，伴随着计算机网络功能的不断拓展与增强，现代人越来越享受计算机网络的便利条件，而且对计算机网络的依赖性也越来越强，现代人生活中，使用计算机网络已经成为不可或缺的重要组成部分。诸如，我们现在可以随时通过各种送餐软件来购买美食、享受美食，而且现在人们的支付方式已经发生了巨大变化，钱包现金已经逐渐消失在现代人的生活中，扫码支付、银行转账等等才是现代人的支付方式。还有，便是网约出租车，现代人尤其是年轻人已经不再是路边等出租车出行了，而是可以直接通过手机软件下单预约车辆，出门即可上车出行。的确如此，现代社会的发展与日益先进的计算机网络技术有着不可分割的紧密联系，计算机网络也呈现出繁荣发展的局面，但是在此过程中，我们也必须要保持客观理性的态度和认知，要知晓现在使用频率如此之高的计算机网络，实际还是存在着诸多安全隐患，而且这些安全隐患随时随地都有可能会威胁到社会的稳定以及每一个人的切身利益，因为计算机网络安全问题而导致的各种利益损失事件层出不穷，为了保证计算机网络价值的稳定呈现和发挥，其必须要对计算机通信网络安全表示出高度重视，如果一旦发生了严重的通信安全事件，其所产生的后果和损失不堪设想。

三、计算机通信网络安全所遭遇到的隐患和威胁

在互联网时代背景下，每天都会有海量新数据出现在大众眼前，而且这些海量数据在传输的过程中会涉及到非常多的敏感信息或者机密信息，比较受关注的便是网络用户个人的信息内容以及企业的机密文件内容、政府机密数据信息等等，这类信息都会因为互联网的使用而被置于一个网络平台当中，通过网络渠道传播，其在享受高效便利传输条件的同时也因此承担了非常大的安全风险和安全威胁。其中一些独具价值的信息数据很容易被一些别有用心的人所窃取和利用，这也是网络安全事件屡屡发生的主要原因。尤其是当今社会中，人们已经越来越习惯网络支付的方式，个人支付信息、个人支付账号、个人支付密码等等都会成为不法分子关注的重点，也会是最具代表性的一种攻击目标。关于当前社会中计算机网络所面临的安全威胁，其可以划分为如下几种类型：

（一）网络传输过程中的安全隐患

1.窃取机密信息

在计算机通信网络当中，不法分子以及一些攻击者所关注的重点目标便是传输过程当中的机密信息内容，一般情况下，不法分子或者攻击者都会选择在某一个传输的关键节点去窃取传输过程当中的信息内容，比如路由器或者网关等节点。而且对于个人使用网络而言，其所涉及到的机密信息在实际网络传输过程当中安全等级都相对比较低，甚至是以明文的形式直接传输到对象手中，所以，对于不法分子或者网络黑客而言，其窃取机密信息难度是比较低的，而且这也是最为常见的信息泄露形式之一。

2.篡改机密信息

在一些特殊的场合当中，不法分子、攻击者或者黑客等，他们进行攻击的目标并不是要窃取信息内容，而是要对机密信息的内容进行伪造处理，要将伪造的信息内容替换掉机密信息的原内容，以达到自己的不良目的。在窃取机密信息的过程中，因为机密信息伪造的隐蔽性特征越来越强，所以很容易因此造成很大的经济损失或者利益损失。

3.伪造授权认证信息内容

当前的计算机通信网络系统，不管进行基础操作还是深度操作，其都需要得到授权才可以进行。不法分子、攻击者或者黑客还有一种方式那就是攻破授权，对授权信息进行伪造，进而便可以获得计算机系统的各项操作权限，通信网络系统运行的安全性也会因此遭到严重威胁。

4.拒绝服务

在一些情况下，不法分子或者网络黑客，他们的目标并不是要窃取传输中的信息内容，而是以破坏计算机网络正常运行为目的，比如比较常见的便是蠕虫病毒等等。这些属于带有恶意性质的拒绝服务表现，这种拒绝服务的攻击行为会瞬时间让整个计算机系统陷入瘫痪，无法正常运转。这种方式不仅会严重影响到工作效率，而且对于一些比较特殊的行业而言，这样的攻击方式很可能造成致命性的打击。

（二）系统方面产生的安全隐患

关于系统方面所产生的安全隐患，其主要涉及计算机软件和硬件的设计与安装工作。一般情况下，计算机专业技术人员会设置针对性的窗口，以方便广大用户更加高效获取和处理信息。设置相应的窗口，虽然可以让广大用户获得更加便捷的体验感受，但是也因此出现了安全隐患问题。信息窗口本身是接受窗口，其是用户用于接受信息以及查看信息的有效路径和方式，所以其随时都可能面临着病毒的侵袭，而且会对整个系统造成严重的安全威胁。在此过程中，如果有病毒进入到计算机系统当中，那么其便很难保证可以彻底消除或者消灭病毒，而且还会对系统内部的硬件和软件都产生不同程度的危害及影响。此外，会有一些比较强势的病毒会趁机入侵到系统当中，进而造成软件漏洞的出现。

（三）人为因素造成的安全隐患

在当前的计算机通信网络安全中，人为因素也是至关重要的一个安全隐患，之所以会因为人为因素而出现安全隐患，其主要原因还是在于自身专业素质。加之人为因素自身的独特性，其随时都会有主观因素的介入和影响，比如会有管理人员因为一时的疏忽大意而造成设备运转出现问题，或者因为自身专业技能的局限而影响到专业设备的正常运行效率。而且人为因素所产生的问题是一种必然现象，是无法完全杜绝和避免的，但因为人为因素所造成的安全隐患，其问题主要还是出在管理人员方面。在相关管理方面，管理设备的缺乏、技术人员的水平不足以及安全意识薄弱等等问题都会直接导致计算机网络通信的安全隐患。针对这些问题，企业应该投入大量的精力去整顿，还给网民计算机网络通信的安全。不论是怎样的因素导致了计算机网络通信出现安全隐患，企业都应该对其重视，从而促进计算机网络通信技术的向好发展。

四、计算机通信网络安全隐患解决对策

（一）加强内网通信安全规范管理力度

关于如何加强内网通信安全规范管理力度，其可以从以下几个方面来着手：

其一，采用安全交换机

广播技术是当前内网传输信息内容的一个主要形式，在广播过程中，传输的数据包内容很有可能被随时截获或者监听，所以，使用安全交换机来更好地保护内网传输的稳定性是比较合适的方式。关于安全交换机的使用，其可以选择使用VLAN方式或者网络分段的方式，如此一来便可以从逻辑层面以及物理层面来对网络资源做出有效隔离，进而便可以很好地增强内网的安全性能。

其二，科学合理使用网关

之所以选择使用网关来保护内网的安全运行，其主要原因在于网关的优势，使用网关，网络数据包的变换并不在内外网络中直接进行，而且内网必须要经过网关之后才可以得到访问网络的权限。如此一来，其自然会对服务器内网计算机网络外部网络起到很好的限制作用。

（二）致力于优化和改善计算机通信系统基本性能

计算机系统系统基本性能是影响计算机通信安全的关键因素之一，因此，在进一步提升计算机通信安全性能的过程中，相关人员要积极致力于优化和改善计算机通信系统基本性能。当前所应用的计算机通信网络在设计方面还是采用了一种相对比较简单的理念和方式，这便为其留存了很多安全风险。关于如何进一步优化和改善计算机通信系统的基本性能，建议其可以从以下几个方面来进行：

其一，要加强对计算机病毒的检测和防护力度，要及时恢复瘫痪网络，并且要进一步优化安全应急处理方案和信息加密管理计划。

其二，要进一步加强对新型安全防护技术的研究与开发力度，要全面增强系统的防护性能，提升系统的安全性，将漏洞的出现概率降到更低。

其三，要设计更多更具针对性和实效性的防护对策，同时健全和完善相关安全管理制度，落实各项检查和监督策略，全方位提升计算机通信系统的安全性能。

五、结语

综上所述，要想进一步促进网络通信的发展和进步，安全的技术是最重要的保障因素之一。相关领域研究人员和技术人员一定要对当前网络安全问题中存在的风险问题给予高度关注和重视，不忽视任何网络安全问题所产生的威胁和影响，以保证计算机网络通信工程建设得以更加全面健康发展。

参考文献

[1]黄磊.新形势下计算机通信网络安全隐患及其对策探讨[J].中国新通信，2020，22（5）：30.

[2]戴志刚.高校计算机网络安全管理存在的问题及对策探讨[J].中国新通信，2020（22）：117-118.

[3]王钰，冯娜，张振宇.探讨计算机网络信息安全问题的成因及对策[J].数字通信世界，2020（4）：72-72.

[4]薛永.试论计算机通信网络的安全问题与应对策略[J].数码设计，2021（12）：20-21.

[5]朱延敏.我国通信业支撑网安全现状分析及对策探讨[J].数字通信世界，2021（2）：126-127.

[6]朱红霞.对计算机网络信息技术安全及对策的探讨[J].数字通信世界，2020（5）：138-138.

[7]齐琪，杨欢.计算机网络通信安全问题及防范策略探析[J].数码设计，2021（1）：1-1.

[8]魏建明.计算机网络通信安全中数据加密技术的分析与探讨[J].通信电源技术，2021（20）：105-107.