机械工程(6)2022,4
ISSN: 2661-3530(Print); 2661-3549(Online)

计算机网络安全问题及其防范措施

黄广锋　江志晃
广东培正学院　广东广州　510830

摘　要：现如今在计算机网络使用过程中安全问题逐渐凸显，而要想提高计算机网络的安全性、可靠性，相关使用人员在进行日常使用时必须做好相应的防范措施，降低计算机网络出现问题的概率，对其病毒、木马程序进行防范，提高网络安全。本文分析了计算机网络存在的一些安全问题，并从技术层面和管理层面提出具体的解决措施，以此来有效应对网络安全问题，让网络具有高稳定性和安全性，对人类和社会的发展起到促进作用。

关键词：计算机；网络安全；防范措施

Computer network security problems and preventive measures

Guangfeng Huang, Zhihuang Jiang
Guangdong Peizheng University, Guangzhou 510830, China

Abstract: Nowadays, in the process of using the computer network, security problems are becoming increasingly prominent. To improve the security and reliability of computer networks, relevant users must take corresponding preventive measures in daily use, reduce the probability of problems in the computer network, prevent viruses and Trojan programs, and improve network security. This paper analyzes some security problems existing in the computer network and puts forward specific solutions from the technical and management levels to effectively deal with the network security problems, which makes the network have high stability and security and promotes the development of humans and society.

Keywords: computer; Network security; Preventive measures

引言：

网络和通信技术的发展给人们的生活带来巨大便利，改变了人们的日常生活方式，但与此同时，网络安全的威胁正在步步逼近，例如网络黑客的入侵袭击与盗取数据信息、网络病毒的发布与蔓延等。尽管人们运用了专业的软件和技术如防火墙、杀毒软件、网络入侵检测器等来避免网络安全问题的出现，但无论是国内还是国外都无法对其完全制止。因此，要及时发现网络安全问题，运用强有力的措施保障网络安全，精确消除潜在威胁，只有这样才能真正让计算机和网络的作用发挥到最大。

1　目前我国计算机网络安全存在的问题

1.1 计算机病毒

计算机网络在使用过程中会出现诸多网络安全问题，尤其是病毒侵袭。病毒作为目前我国计算机网络在使用过程中最大的安全隐患之一，它主要是通过恶意程序来对计算机系统进行破坏，通过代码导致系统出现问题，脱离运行，如崩溃、破坏等[1]。虽然病毒并不能构成较大的危险，但是在软件安装过程中会对整个程序产生严重影响，如果使用人员没有及时对其进行发现并处理病毒，它会以极快速度进行蔓延，对其余软件产生影响。病毒潜伏性较高，很难将其进行清除，无疑加大了计算机网络出现问题的概率，因此相关使用人员在进行计算机使用过程中必须做好病毒查杀工作，从而降低系统感染病毒的概率。

1.2 黑客攻击

在计算机网络运行中，还普遍存在着黑客攻击及木马程序等安全问题，其中黑客攻击主要包括破坏性攻击及非破坏性攻击两种，前者对计算机系统造成破坏的同时，对数据信息进行窃取，通常采用密码破译、后门程序等多样化的攻击手段；后者会对计算机系统的正常运行造成影响，通常采用窗口弹跳及信息炸弹等方式表现，

不会对系统内部信息数据等进行窃取破坏。另外木马程序通常会利用伪装方式引导用户进行点击下载，一旦下载安装，木马程序编制者能够利用用户所安装的木马程序对其计算机系统进行入侵，可实现对系统中所有内容的复制、查看、损害、删除等操作。

1.3 计算机自身系统漏洞

开放性是计算机系统最明显的特点，正是因为这一特点，给计算机用户带来了极大的便利，同样也因为这一特点，为计算机网络安全带来了巨大隐患。例如，计算机网络允许用户自主安装程序，或进行文件传输，但大部分程序与执行文件，均是人为编写的，只要是人为编写势必会存在一定漏洞，这些漏洞就容易被不法分子利用而入侵计算机网络，或者这些漏洞会导致计算机防护系统出现缺陷，而降低网络安全防护，增加计算机网络安全风险。而且，计算机软硬件系统的应用也面临一定安全隐患，目前计算机最常见的系统是Windows系统与Linux系统，虽然应用比较普及，但也不意味着完全安全，这些计算机系统也存在一定的安全漏洞。此外，用户自身操作也会导致一定安全隐患，部分用户缺乏安全意识，未根据相关规定采取计算机网络安全防护措施，或者在实际操作中违法相关规定，均会导致计算机网络安全隐患。例如，未设置计算机登录密码、电脑中账号设置成自动登录模式、密码通过于所有账号、计算机中未安装有效杀毒软件等。这些均是计算机用户会出现的一些不规范操作，给病毒或黑客提供了可乘之机，影响计算机网络安全。

2 计算机网络安全问题的防范措施

2.1 使用硬件加速提高计算机网络的安全性

公司、校园或家庭的网络中都有大量的数据传输，这些数据流量一般在效率高的网络节点之间传输，而在这之中会存在大量的垃圾数据，这些垃圾数据会伴随着传输数据传输，不利于网络节点设备的使用并占用带宽。如果使用硬件加速的方法，可以充分利用用户GPU提供的硬件加速功能，让其执行更多具有灵活变通性的其他功能，将性能等级从每秒百兆比特提升到每秒吉比特。硬件加速主要是用硬件模板替代软件算法以充分利用硬件所固有的快速特性，使网络系统的过滤品质与吞吐量实现升级，以此对数据包进行准确处理。这样既能保持计算机的高性能水平，又能对软硬件的安全性能进行保障，提高计算机网络的安全性。

2.2 防火墙技术

在网络技术高速更新背景下，防火墙技术在计算机网络安全管理中的应用也越来越广泛。在相关技术应用中，防火墙可以帮助计算机最大限度地避免受到病毒的侵入，为计算机网络内部安全提供有力保障，尽可能减少外部风险给网络安全带来的不利影响。防火墙技术在具体引用中，需要对其安全协议内容做出充分考虑，这样不论是哪一类信息在进入计算机之前，都要得到协议的允许，才可以通过防火墙[2]。若一些存在安全隐患的信息想要从防火墙通过，防火墙会立即强力阻隔这些信息，能够有效避免外部病毒利用脆弱的协议来给信息网络带来攻击。此外，记录网络访问也是防火墙不可忽视的一个功能。结合相关记录可以让计算机系统获得安全性更高的统计数据，同时科学判断内部数据，以确保系统中存在的问题可以被及时发现，同时发出警报。

2.3 加密技术

结合网络数据信息来科学引用加密技术，可以有效提升网络安全水平，同时使得计算机网络安全管理有效开展。加密技术主要是引用数字加密来进行算法加密，简单来讲，就是通过特殊技术的合理引用来妥善处理计算机网络中的一些明文信息，让其成为一种不能直接进行窃取的密令文件。这些文件可以有效地阻碍一些非法用户的密码破译行为、数据窃取行为，能够促进数据信息保密性显著提升。将明文转变成密令文件这一过程其实就是加密的过程，反之便是解密过程。密钥简单来讲就是在加密、解密中随意转换参数值。另外，在加密技术上，要想促进网络安全性的进一步提升，还可以实现对数据流技术的科学引用，以此来为各类信息提供有力保障。加密数据流其实就是计算机中的一个字或者是字节。在计算机网络中，作为加密技术，数据流具有的破译难度更大，且具有多样性的位移方向。为了多重保护计算机网络中的数据信息，还可以在引用数据流加密技术的基础上，使用xor操作，以此来进一步提升信息网络的安全性。

2.4 加强网络监控工作

加强网络监控工作，是提升计算机网络安全性的重要举措。具体来说，网络监控工作即重视计算机网络的入侵检测，通过网络通信技术与推理技术等，对网络入侵情况进行实时检测，一旦发现有入侵行为，立刻判断入侵行为的合法性，如果判断为非法入侵，立刻禁止该行为并报警。通过加强网络监控，可以显著提升计算机网络的安全等级，对计算机入侵情况进行全方位监控。在现阶段的网络监控分析技术中，统计监控技术与签名监控技术是关键，其中签名技术是用来分析计算机网络

是否被攻击，而统计技术则是对计算机网络使用情况的实时监控。总而言之，加强网络监控工作，可以显著提升计算机网络的安全性。

2.5 病毒入侵信息及时掌控

在计算机网络运行过程中，可利用专门针对计算机网络入侵信息进行实时获取，使计算机网络病毒入侵、信息被盗风险最大限度地降低，使信息被盗或被破坏风险最大程度减少，使网络安全性有效提高，同时应对信息监控系统加强建设，对最先进的技术加强应用，使网络安全性提高。其次通过监控技术的应用，在计算机入侵信息监测过程中，加强网络技术、推理、统计等技术的全面应用，其中通过签名分析法的运用，对网络信息进行监测；通过特征分析方法的应用，能够对计算机系统的弱点进行全面了解，在此基础上对系统加强实时监控，并通过统计学方面知识的运用，对可能危害计算机系统的各项危险因素进行分析、统计和计算，一旦计算机出现异常状况时能够及时发现和处理，使计算机系统安全性提高。

3 结束语

总而言之，如今我国已经全面进入信息化时代，计算机网络使用频率以及效率得到大幅度提升，而计算机网络安全问题也逐渐凸显，这对于计算机网络正常使用会产生较大的影响，对企业、社会、经济发展都有一定的阻碍作用。因此如何提高计算机网络的安全性、可靠性是每一位网络使用人员以及管理人员都应该思考的问题。相关工作人员必须对网络安全问题引起重视，做好相应防范工作，根据不同安全问题产生机制制定相应的防范措施，从而营造出良好的网络环境，让网络技术能够更好地服务于大众。

参考文献：

[1]李龙腾.计算机网络安全问题及其防范措施[J].计算机与网络，2021，47（11）：53.

[2]周雷干.计算机网络安全问题及其防范措施[J].网络安全技术与应用，2021（05）：162-164.