基于网络通讯信息安全的保障研究

王 伟 李 宵
陕西麟北煤业开发有限责任公司 陕西 宝鸡 721505

摘 要：在计算机科学技术飞速发展的今天，计算机网络通讯技术在计算机上的运用，已深入到人们生活中的方方面面。我国计算机网络的发展速度较为迅速，但近年来网络信息安全事故的频繁发生，也使得人们对网络安全的重视程度逐渐提高。国内对计算机网络信息安全的研究并不特别透彻，尽管有了一些防护策略，但这些策略并不能适应现阶段计算机网络技术发展所带来的需求。为此，本文主要对计算机网络通讯信息安全防护策略进行了分析，目的在于为有关人士提供一些借鉴与帮助。

关键词：网络通讯；信息安全；保障

引言

当代，计算机时代、网络信息时代、大数据时代、计算机与网络不断丰富着人们的生活并为全社会高速运转奠定坚实基础。但是计算机网络造成的威胁却很难忽视，这主要是由于许多重要信息都存储于计算机与网络中，一旦发生泄露就会造成巨大损失。再加上计算机与网络自身存在着容易被攻击到的漏洞，尽管近年来人们对计算机与网络安全的重视程度在不断提高，但是，从当前的情况看，计算机及网络安全仍受到威胁，计算机及网络的安全防护还存在一些急需解决的问题，因此加大力度保障计算机网络安全是当务之急。

1 计算机远程网络通讯技术的特点

计算机远程网络通讯技术本质上是计算机在不同端口间进行信息的相互传递，在计算机网络日益发展的今天，计算机网络通讯技术已经被广泛应用。古代人类以烽火和信鸽为载体进行信息传递，电问世后，人类通讯的发展又向前跨出了巨大的步伐，产生了以电磁波为载体进行信息交流的无线电波通讯以及以电流变化为载体进行信息交换的电话通信，两大通讯手段极大地影响着人类社会活动。而且近年来伴随着科技的快速发展，计算机远程网络通讯技术已经深入到各个行业中，掀起了通讯手段所导致的社会文明的变革。与传统电磁波通讯及电话通讯相比较，计算机远程网络通讯具有简便，费用低廉，抗干扰能力强等最显着的特点。

计算机远程网络通讯技术和计算机之间有着密切的联系，而这正是其重要的特征，正因为有了这种特征，计算机远程网络通讯技术刚刚深入到生活中的方方面面。由于计算机远程网络通讯技术和计算机之间的联系非常密切，这样就能够通过计算机对通讯信息进行快速的处理，因此就衍生出来很多的相关行业，例如网上银行，网上购物和电子支付等等，这类功能是计算机对通讯信息进行有效处理的结果。

2 网络通信信息安全的重要性

网络有很强的开放性与普遍性的特点，它作为大众化平台，每个人都能参与其中。网络所具有的灵活性、开放性在带给人们更多方便的同时也给某些不法人员利用网络从事违规操作、盗用信息等行为创造了良好的契机。网络通信发展中存在着种种安全问题，网络黑客和病毒均对网络系统安全性造成更大威胁，当入侵网络系统时，用户信息将被删除，破坏和篡改，造成信息安全得不到有效保证。因此网络通信中信息安全有着极其重要的地位，这就要求我们必须要加强对网络通信质量进行提升，保证信息的安全，这样才能够对信息交换安全起到重要保障作用。网络通讯安全感念由诸多因素组成，在广义国际化层面上，网络通讯信息需符合可用性和有效性、完整性与保密性才称得上安全，一般网络通讯安全都是指从网络的固有特征、根据网络信息安全技术、以及对侵犯网络硬件系统的解决办法等方面提供系列服务。

3 网络通讯中常见问题

3.1 网络通讯技术的故障原因

网络通讯技术中常见的故障包括以下几个方面：一是不能上网，浏览器不能浏览页面，局域网中的计算机很难分享信息技术等等，其中最重要的就是计算机硬件和软件出现了问题。计算机硬件故障多表现为设备故障，线路被扰乱，很难正常通信，或由于人为原因导致网络连接不正确，使网络通讯技术不能正常使用。通过对故障原因的探究，发现计算机硬件故障和设备的供电电源以及供电线路都有一定的关系，一旦供电电源或者供电线路出现问题、供电电压的不稳定性是出现了不能

接入网的情况。二是端口失效。现阶段计算机网络通讯技术采用光纤端口和RJ-45端口两种端口，其中一旦两者发生破坏，会造成网络通讯不能正常工作。集线器和路由器是计算机中的组成部分，二者发生损坏的原因多为使用过久或者受到外界因素的影响。主机模块故障大多是由于操作人员错误或者电源供电不稳等原因造成的。软件故障包括软件安全故障和网络设置两大类型，通常软件故障比硬件故障更难检测。软件故障后用户很难正常浏览页面，网速减慢，造成软件故障的原因有交换机组态不当，电脑被病毒侵害和主机网络地质参数设置不够科学等。

3.2 安全意识薄弱

以上问题例如网络病毒的传染与扩散，用户个人信息泄露等等都是危害网络通信安全性的客观因素。用户安全意识淡薄给数据信息安全带来的威胁，是网络通信安全面临的主观影响因素。安全意识淡薄，意味着用户对于网络信息安全没有一个正确的认识。实践中安全意识淡薄表现为如下行为方式：利用计算机设备故意封闭防火墙，公共场所接入不明WiFi、对网络上不健康网站进行浏览，对来源不明二维码进行随机扫描，对安全状态不明网站进行链接等等，都存在着一定几率将用户自身数据信息泄露出去，从而导致不同程度上经济损失。

4 网络通讯信息安全的保障实施策略

4.1 加强网络通讯的正确意识

网络通讯信息安全保障方法之一是强化网络通讯正确认知。对于网络通讯使用者来说，网络通讯对信息安全最大的威胁就是使用者本身对网络安全没有一个正确的认识。在当前信息化时代下，人们天天要使用网络，但本身并不具备对网络通讯信息安全的正确和理性认识，所以相关工作人员一定要加大力度对相关领域进行宣传。比如不管是办公电脑还是私人电脑，一定要安装高效的防病毒软件和给操作系统打上补丁，严禁随意安装和下载未知软件系统，特别要重点防范下载过程中非法软件侵入。

4.2 提升系统配置

有必要对目前网络通讯交换系统控制和配置进行升级，使网络连接核心设备变得更先进，从而带动整个网络通讯效率的提高，强化网络通讯的管理，对网络通讯系统实施全方位的监控和排查。发生数据异常时，将数据进行全方位的解析，解析出过程中所面临的安全风险并制定出行之有效的解决措施来改善现存问题，确保各系统的运行安全，抵御外界因素影响对通讯信息进行防护，增强网络通讯信息安全。通过对网络通讯信息交换机加强防护，使网络系统更全面地进行网络通信信息的整体把控，及时得到网络通讯信息中的数据信息并合理地调整其运转方式。保障物理网络安全和预防因物理介质和信号辐射带来的安全风险。使用网络安全控制技术的联网单位应当使用防火墙和IDS保护网络安全。制定系统安全技术措施、利用漏洞扫描软件对系统漏洞进行扫描、封闭不必要服务端口等。

4.3 加强计算机网络的加密措施

将数据加密技术运用到网络通讯中，可以有效地加快数据通信，网络平台应用安全系数，保证双方通信处于安全环境中，保证数据不会被盗而损坏。计算机网络加密就是将明文转化为密文，从而达到对网络中数据，文件及控制信息的保护功能，而加密对应解密即密文还原为明文。目前加密数据可采用如下三种方式进行传输。其一是节点加密。节点加密所采用的方法就是给发送路径上节点机发送的消息进行加密，和其他加密方法不同，节点加密并不能使发送消息在发送过程中显示为明文，利用节点加密的过程中，它首先会将收到的数据信息进行解密，再利用一个安全模块内的另外一个密钥对解密明文进行加密，这是与链路加密不同的地方。另一种是链路加密。链路加密主要指网络节点之间所增加的密度，即在传输过程中对信息持续加密与解密直至数据信息被传输到真实的信息接收端，但是对于信息发送端和信息接收端进行防护并不进行处理，仅仅是针对通信传输途中信息安全进行防护的一种加密类型，这种加密算法存在的不足在于信息一般都以明文的形式呈现于节点中，导致信息易受到攻击。端到端的加密。端对端加密不同于另外两种加密方法，端对端加密的主要过程就是数据信息在发送端和接收端的整个传输过程中以密文的形式出现。即在传输数据信息时，并在到达接收端之前不采取解密的措施，从而使数据信息能够在传输途径上得到防护，即使消息在传递过程中存在节点断裂，但并不会导致消息外泄。该加密方式还存在不足之处，即发送端与接收端之间无法隐藏传输数据信息，为提升数据信息传输更安全，可将链路加密与端到端加密同时进行，从而确保信息传输更安全。

4.4 加强网络认证体系结构

为了针对具体情况建构相应的控制和处理机制，系统管理人员可让用户设定两种访问权限，当用户利用网络资源，大多数用户都是把用户名和密码单独存放，以防密码遗忘或者遗失，这样就可以对用户信息有一定的保护效果，以免个人信息被盗。但是此法仅在短期内见效。在不断地进步发展之后，系统内部的各种连接都

遭到了袭击，导致网络通讯变得不够稳定。其次，采用安全令牌等辅助校验方法，这一方法可使数据处理更加完整可靠，校验结构层次大大提高，充分发挥控制结构的有效性，并坚持研制结构与技术同步发展的原则。在当前阶段，指纹和刷脸验证属于一种比较新颖的认证方式，能够有效地避免密码受到他人的复制和篡改，切实地保障数据信息安全。

4.5 提高网络通讯中的防火墙系统

防火墙系统为确保网络通讯信息安全提供了主要途径。为了确保通讯网络的信息安全，防火墙系统在其中扮演着重要角色，它能够检测出数据流失的程度，规避病毒入侵软件，防止不法分子的监听，从而真正维护个人信息安全。但是建立防火墙并不是行之有效的解决办法，必须定期进行更新，安装在软件中的扫描病毒插件和杀软件也应及时进行更新，从而屏蔽病毒入侵，达到增强信息安全性和给人们营造一个优质通讯环境的目的。

4.6 注重病毒防护技术应用

网络活动中木马和病毒已成为网络信息安全的毒瘤之一，计算机网络病毒和木马每年蔓延所带来的危害是不可估量的。防病毒和反病毒问题是信息安全领域中的一大难题，因为计算机病毒具有隐蔽性，传播性和破坏性等特点，可以通过各种媒介和方式进行传播。反计算机病毒技术包括病毒的识别，检测，明确和免疫预防等方面的内容。传统病毒防治都是被动的，而随着计算机网络技术的进步，下一代防病毒技术能够在病毒扩散和暴发之前改善和识别病毒并达到主动防御。传统的病毒防治是比较被动的，而随着计算机网络技术的发展，新一代云计算防病毒技术能够在病毒传播和暴发之前就预先进行识别和清理，从而达到主动防御的目的。加强网络漏洞扫描与修复对防范恶意攻击者具有良好作用，而网络安全性扫描仅是提升通信网络信息安全水平的重要举措。并可根据扫描到的漏洞，下载适当补丁，及时修补网络，继而确保通信网络信息安全。对于网络信息安全制定出合理且及时的应急措施同样非常必要，可以保证当网络信息安全出现问题时可以得到及时且有效地处理。现在对通信网络中存在的信息安全问题应该做到防范为先，不仅需要强化提前防范，还需要对出现后采取相应的措施进行处理，从而确保网络信息安全性。制定口令管理制度以避免系统口令泄露及暴力破解。

4.7 加大对网络的监管

一是从立法层面上看，政府部门在增加网络信息安全立法过程中，还需对当前阶段网络信息安全法律体系做出必要改进，由于网络信息技术发展迅速，在当前阶段法律法规中对很多问题都不太重视，所以在当前网络安全法律法规中仍然存在很多漏洞，基于这一现状，立法部门须及时查漏补缺。另外政府部门也要建立一个健全的网络规制机制，在这一阶段，尽管已有相关的机构来规制我国网络信息安全，但这种规制机制具有很大的不合理性，监管漏洞和重复监管等问题频发，使我国网络信息安全稳定问题备受困扰。基于这种现状，政府部门有必要重新设立网络信息安全专门机构。

结语

从整体上看，针对网络通讯存在的信息安全问题应该采取相对有效的策略并真正落实到位。信息安全策略，从概念性分析，主要是指为了确保提供某种等级的安全保护而需要遵循的行为准则。网络通讯的信息安全不可能仅仅依靠先进技术来实现，还必须依靠一些安全管理和相关法律约束来实现。具体而言主要有以下几个方面：采用一定的智能手段，使得在传输过程中可以主动地识别涉密信息与数据并且可以及时地进行加密操作，该系列行为不需要人员介入，从根本上消除了机密被泄露、遭恶意篡改等问题。尽管如今计算机已经运用于社会各个领域中，但是网络还是一个新事物，很多行为都不能可依，以致于网络犯罪钻空子，所以，有关部门应做好有关法规的健全，制止网络犯罪行为。

参考文献

[1]张佳.基于网络通讯信息安全的保障研究[J].信息与电脑(理论版),2019(07):219-220.

[2]郭国林.基于网络通讯中信息安全的保障研究分析[J].中国新通信,2017,19(06):37.