计算机网络信息安全风险及解决方法

吴秀娟　荣　曦
济南市气象局　山东　济南　250000

摘　要：科学技术迅速发展背景下我国网络信息技术得到显著提升，为我们工作和日常生活提供很多方便，同时也造成许多互联网安全隐患，直接威胁着我们的日常工作，甚至造成很大的损失，所以我们应该正视这一状况，选取正确的入手点，提高互联网信息的安全。

关键词：计算机网络；信息安全；解决方法

1 计算机网络信息安全的风险类别

1.1 网络通信线路和设备的缺陷

实现通信的超高速和全面服务，关键在于各层次数据传输、各种阶跃的传输方式的相互转换和业务的逐步发展，在一般的网络数据传输环境中，首先通信的安全性是很重要的，其次可靠性也非常关键。能否安全、平稳，将直接决定通信线路的通达度。但目前，通信线路及其设施的安全风险通常由以下几点所构成：电磁泄露、设备窃听、端口访问，以及网络攻击。当通信线路和电子设备缺陷或裸露时，信息系统设备在工作过程中接受地线、电源线、信号线、寄生电磁信息以及谐波的照射，在这些条件下就产生了最终的电磁泄露现象。

此时，网络攻击者就能够通过电磁泄漏技术来捕捉并解密无线网络的信息，以便于比较方便的获得传输信息。在信息发达的网络时代，阻止网络拦截的网络安全技术已是一种成熟的网络风险预防手段之一，它主要利用网络截获装置对不法犯罪分子实施非法截获的信息捕获。在网络入侵所伴随的以太网中，口令被窃听，机密信息被截取，网络攻击者还通过异步串口连接共享机可以通过终端连接的方式连接到终端。在完成的终端之间以及前身与其他终端之间，攻击者的合法终端欢迎欺诈终端，并在与合法用户相同的计算机通信操作下发布欺诈信息。随着这些信息和机制的不断演变，一些“垃圾信息”、“电子邮件炸弹”、“病毒马”、“网络黑客”等威胁着越来越多的网络安全，其中以网络攻击最为重要，是威胁的其中之一大来源。

1.2 软件存在漏洞和后门

网络战并非遥不可及的未来，事实上，网络战已经切实存在在每个人的生活中，并且变得非常普遍，在目前的网络中，网络战已经无处不在，漏洞也到处都是。软件的漏洞和后门也给这些电子武器商人们带来了方便之所，从而导致网络信息安全大战无处不在。在这个技术为王的年代，人们的整个日常生活，包括商业和医学，还有我们每个人的工作轨迹，包括政府、大学，甚至一切的应用软件都开始被大数据所充斥着[1]。

此外，网络病毒利用各种手段进行在我们的电脑中，他们从用户的个人信息、私密资料或者是我们每个用户的银行账号资料中盗取我们的数据并以此获得欺诈性收益。一旦软件端口不受到充分的安全性约束，就有可能会允许各种形式的攻击者在未获取许可的前提下登陆并入侵网络，从而损害互联网生态。

1.3 人员风险

网络信息安全问题必须由人来控制和影响。从系统用户的角度出发，系统用户的保密思想不强，关键信息没有加密，如果密码保护强度低，文档共享没有经过必要的权限控制都是造成计算机网络信息安全风险的重要原因。从技术人员的角度来看，技术人员的工作不熟练或不负责任，因此有意或无意地破坏了网络系统和设备的保密措施。从专家的角度来看，专家利用工作的便利，以欺诈手段进入系统，以欺诈手段获取信息。从侵权人的角度来看，侵权人利用系统的端口和传输介质，通过窃听、捕获、解密等手段窃取机密信息。因此人员网络信息安全防空素质的高低也将影响网络信息安全。

1.4 管理风险

网络安全管理不仅能有效地确保网络安全系数的专业度，也能在一定程度上保护个人用户的所有数据信息，但由于管理问题，网络信息安全问题是有可能发生的。一是安全管理的体系不健全，这反映了管理者对网络信息安全重视度不足；二是监管机制不健全，技术人员不齐，安全警觉，缺乏有效监管；三是教育培训不到位。缺乏对用户的安全知识教育和对工程师的专业技术教育[2]。

2 加强计算机网络信息安全的方法

2.1 信息加密技术的应用

第一，应用加密是保证计算机网络安全的重要措施，也是信息传输安全的重要保障。在信息加密技术的具体应用中，数据加密、数字签名以及密钥交换等，都能够有效提升网络信息的安全水平。将密码分析学应用到具体的实践中，能够形成更为安全的机制，提升网络系统的抗风险能力。

第二，数据加密与解密技术的应用。在加密算法应用过程中，需要重视密钥、公钥以及散列算法的作用。在实际网络中，经常选择的加密方式有端到端的加密、链路加密以及节点加密等。在解密技术的应用过程中，其主要目标在于寻找算法的漏洞，基于设计的弱点对密码进行破解，并根据解密的情况做好加密设计的完善工作，进一步提升网络的安全性。

第三，认证技术的应用。认证技术的应用主要是对各类数据的传输过程进行集中验证，通常情况下可以选取信息认证和身份认证两种方式。就消息认证实践的现状而言，通过认证技术的应用能够进一步提升信息传递的完整性。并对信息是否进行过第三方修改进行集中检测。消息的认证包括安全散列函数、消息认证码以及数字签名等内容。身份认证主要指的是多个用户向系统传递个人消息后，在进行身份验证和识别的过程。

2.2 访问控制

对于计算机网络系统的防护，需要提升对访问控制的重视程度，借助有效的身份认证方式，对资源访问以及系统的限制进行规定，从而提升对网络资源的控制水平，确保用户能够根据自身的实际情况对相应的数据资源进行安全访问。通常选择的访问控制技术，会涉及到角色访问和自主访问等内容，借助自我访问能够进一步做好资源保护工作，从而实现权限的隔离。但资源的分散性比较强，因此管理起来存在一定的困难。对于角色访问而言，就是将不同角色与其访问的权限进行连接。在具体管理过程中，需要结合实际情况，提升管理的规范性，及时做好用户权限的增减工作，从而为用户的使用提供安全稳定的网络环境[3]。

2.3 防止黑客入侵计算机系统

有很多的黑客尽管想要攻击计算机网络系统，但是在攻击网络系统时还需要满足很多的条件，一般是通过暴力破解的方式或者采用其他的渠道获取计算机用户的身份认证。用户在使用计算机的过程中，只要做好相应的防范措施，就能够杜绝大部分黑客的攻击。

近些年，有很多的不法分子会通过互联网盗取用户的资料，这就给用户带来了很严重的经济损失以及隐私的泄露，还有一些黑客会利用某些计算机端口，盗取计算机用户的密码以及账号，破坏计算机用户的系统。因此，计算机用户在平时使用过程中，需要定期或者不定期的更改密码，要使用好防火墙技术，做好隔离措施，控制住网络对计算机的访问渠道和访问权限，这样能有效防止被黑客攻击。

2.4 及时做好文件备份及垃圾文件的清除

备份是保证计算机数据安全的最有效方法之一，系统和数据都要进行必要的备份，以防系统发生故障时可以迅速恢复系统和相关数据，减少不必要的损失。对于用户计算机里面的重要文件，需要用户细心地拷贝到其他不会接触到互联网的储存设备中，这样可以防止病毒在入侵到计算机之后格式化，造成重要文件的丢失。

并且还要对电脑中的文件做好相应的区分，对于一些可疑的文件，用户不要随意地去点击，这种可疑文件有可能是木马病毒进行伪装之后的文件，这种可疑文件一旦运行起来就会给电脑系统造成很大的伤害。用户对于计算机中的一些垃圾文件也需要定期或者不定期地进行清理，这样能在一定程度上提高计算机的运行效率。此外，用户还需要做病毒的入侵检测，对于一些恶意的病毒攻击要使用防火墙进行及时拦截，这样能保证用户计算机网络的安全性。在检测的过程中一旦发现有网络攻击的现象，就要立即采取解决措施，比如硬盘格式化、断开网络等方法将用户的损失降到最低。

2.5 增加访问控制的难度

用户在使用计算机进行网络活动时，需要在访问时输入相关的账号和密码，这样会加强访问的难度，但是也能在一定程度上确保信息的安全。用户在设置账号及密码时，需要尽量将账号和密码复杂化，密码应使用大、小写英文字母、数字加特殊符号进行混合，在一定程度上加大密码破解的难度。与此同时，还需要尽量避免使用一些比较简易的密码，比如说重复性的数字、连续性的数字、生日、电话号码、身份证号码、学号以及自己、父母、爱人和孩子姓名的汉语拼音等[4]。

在大数据环境下，封闭的方法并不是最明智的应对网络信息安全风险的办法。信息和数据的共享对于一个公司、一个地区、一个行业的长期增长是必不可少的。在这种情况下，网络层面的高效数据共可以实现资源的高效利用并防止资源浪费。但由于互联网本身的开放性，无法有效保证应用平台“云计算”在数据信息共享过程中的安全性，在利用互联网共享信息的过程中，在易用性，信息共享的威胁，特别是在现在竞争日益激烈的社会，从一些不法分子那里窃取信息，通过数据获取自己不正当利益的现象越来越多，所以，人们在使用

大数据平台时必须加强“云计算”服务平台的监管和管理，必须是“云计算”信息资源共享的过程，“云计算”服务平台将防止非法入侵和数据窃取的情况。

结束语

综上所述，为有效地提高计算机安全工作，并保障使用者的隐私权与安全，就必须在用户使用电脑的过程中进行对计算机的安全保护工作。用户作为电脑的用户，就必须增强自己的安全意识，在使用电脑的过程中，切勿随便浏览不明链接，不能随便使用不安全网站，合理运用各类安全管理手段，包括防火墙等，如此方可保障客户的安全。

参考文献

[1]段华斌.论大数据背景下计算机网络信息安全风险和解决对策[J].信息记录材料，2021，22（04）：235-236.

[2]常燕.大数据背景下计算机网络信息安全风险和解决对策[J].信息记录材料，2021，22（04）：198-199.

[3]宋泱瑾.大数据背景下计算机网络信息安全风险和解决对策研究[J].电子元器件与信息技术，2021，5（01）：26-27.

[4]梁德华，万欢.浅析常见网络威胁及其防范方法[J].成才之路，2010（03）：88.