计算机网络信息安全及应对策略探究

吴开阳
（中南林业科技大学，湖南 长沙 410004）

摘要：伴随着我们国家的经济和科学技术的持续发展，我们的计算机网络技术正处在一个快速发展的时期，但由于网络环境的开放性，计算机网络信息亦面对着极大的安全性难题。在此背景下，如何有效地保护计算机系统的网络信息安全是当前计算机系统中一个亟待解决的问题。本文首先对计算机网络信息安全的基本含义作了初步剖析，对其所采用的几种关键技术进行了详细的剖析，并对目前计算机网络安全中所出现的问题进行探讨，提出有针对性的对策。

关键词：计算机；网络信息安全；应对策略

在计算机网络信息安全方面，最重要的问题就是，用户的计算机网络系统中所保存的数据、硬件，以及相应的程序等是否会被外部的力量给破坏，甚至是被泄露，造成故意或无意的破坏。在计算机不被未许可和未经授权的访问和使用情况下，要如何才能确保计算机网络系统的相对安全，是相关人员需要思考的问题。另外，就电脑网络的安全性而言，不同的使用者也有不同的需求，既可以确保用户的私人资料不被泄漏，又可以确保用户的私人资料不被其他用户所获得和利用。对于公用网管而言，只要不让别人获得网管权限即可。对企业和国家信息的保密部门而言，网络信息安全就是将数据和信息安全地存储在特定的地方，不会因为外部的攻击而引起数据信息被破坏或泄漏。

一、安全技术概述

（一）防火墙技术

简单实用，在不对原来的网络应用系统进行修改的情况下，可以满足一定安全需求的防火墙是一种重要的网络安全技术，其不仅可以对流出的 IP 包进行筛选，还可以对外界的威胁 IP 进行拦截，进而对内部的网络进行保护。防火墙最大的优势在于它能够对从外面到里面以及从里面到外面的一切信息进行筛选，只有那些满足条件的信息才会被防火墙释放出去，而那些不满足条件的信息则会被防火墙拦截下来。除此之外，它还具备防入侵的功能。但是要注意的是，在设置防火墙的条件下，公司或者企业在内部和外部的网络连接中，必须要有数据保护功能，而在内部和外部的网络中，由于防火墙要过滤内部和外部的数据，所以就必须采用其他的方法来实现，从而导致网络中的消息传递速率的降低。对于用户而言，经常会采用一种十分便利和实用的防止计算机中的信息被入侵的个人防火墙技术，可以有效地监视及管理系统，防止病毒、流氓软件等通过 Internet 进入自己的计算机，或是自己计算机中的信息在无意中向外扩散。

（二）数据加密技术

在信息化社会中，信息给每一个人带来便利的同时，也会给每一个人带来危险，甚至带来危害。例如，在相互竞争的公司和企业之间，信息的泄露会带来很大的损失，因此就需要一种强大的技术来保护数据，防止信息数据被盗或者被篡改。另外，对于数据的加密和解密，也是一种很容易掌握的技能。资料加密是一种利用资料加密、解密等手段，来限制资料使用者对资料的访问，从而达到资料安全的目的。两种主要的密码体制，一种是采用单密钥的对称性密码体制，另一种是采用“公匙”与“私匙”成对的不对称密码体制。

（三）虚拟专用网技术

现阶段，最先进、最成功的解决信息安全问题的技术之一就是虚拟专用网技术。该技术在数据传输中进行了加密和验证，它的使用费用比传统的专线方式要低，而且具有更高的安全性。虚拟专用网的用途非常广泛，我们平时在家中使用的拨号上网，在办公室办公时使用的内部网络都是虚拟专用网。VPN 采用密码与身份验证相结合的方式，可以对网络中的数据进行有效的保护。

（四）安全隔离技术

众所周知，由于计算机技术的不断发展、创新，现在新型网络攻击应运而生，这就需要开发高安全性的防新型网络攻击的技术，而安全隔离技术是把危险的信息资源隔离在外面同时保证内网的安全。

（五）身份认证技术

登录我们的 QQ，微信，百度文库、淘宝等网站，会发现如果想成为会员，需要对应的会员账号与密码，方可进入页面，必须要有一个使用者名称和一个口令，只要你把这个口令给了我们，我们就可以在一些网站上找到你想要的东西，比如语音、虹膜等等，这些需要经过验证的技术叫作“身份验证”，其实质就是利用被认证方所知晓的资料，让被认证者对你的身份进行验证。

二、计算机网络信息安全存在的问题

1. 就当前国内的网络信息技术来说，尽管它已被广泛应用，并具备了充分的开放性与公开性，但仍存在着一些缺陷，这就造成对计算机网络信息安全无法进行有效控制，难以对某些网络攻击和恶意破坏进行及时阻止。并且，当前我国网络信息安全相关法律尚不健全，网络信息安全法律并未对某些网络行为作出明确的规定，从而导致网络中存在着破坏和攻击的现象。

2. 网络计算机用户使用不当。当前，很多网络计算机用户在进行一些网络行为和活动的时候，并没不具备较强的网络安全意识和自我防范意识，依然抱有侥幸心理，没有充分认识到网络安全问题的严重性，有些用户会把自己的私人信息和资料上传到网上，而不知道这样极易被损坏或偷走。此外，网络病毒和黑客还可以突破用户的安全保护，从而给网络用户带来了巨大的损失，包括经济和政治等。此外，有些使用者在设定网路账号与密码时，只是使用简单的个人资料来设定自己的账号与密码，这样就很可能会在账号与密码中泄漏自己的私人资料，这也导致了一些人的私人资料被盗取，以及一些人的权益受到了侵害。

3. 网络黑客的恶意攻击。随着计算机网络的发展，有些罪犯会对网络信息技术有很好的把握，他们抱着一种侥幸的心态，以为自己实施了一系列的破坏活动就不会被发现，所以他会用自己的技术来实施新的网络攻击。一般情况下，黑客都是利用用户的计算机网络安全的弱点，入侵到用户的电脑系统，然后盗取或者破坏用户的信息。

4. 计算机网络病毒的传播。在计算机网络信息安全领域，计算机网络病毒问题是一个非常棘手的问题。它的传播过程比较隐蔽，危害比较大，并且其传播路径比较广泛。一般来讲，网络病毒是可以通过某些网页或软件程序来传播的，并且网络病毒会隐藏在有关的程序或文件中，然后利用某些伪装的手段来吸引用户下载，一旦被感染，就会被入侵。一旦被用户触发了网络病毒，那么用户的网络系统就会遭受到巨大的破坏，严重的话还会导致整个系统陷入瘫痪，在这种情况下，用户根本就没有办法去阻止，并且还会导致个人信息资料的损坏或丢失。并且从目前的情况来看，网络病毒具有很强的隐蔽性，因此会对网络信息产生很大的危害，给用户带来很大损失。

三、计算机网络信息安全及应对策略

（一）提升个人安全意识

保护好计算机网络中的信息安全，是每个使用者都应高度重视的问题。首先，我们要加大宣传力度，让每个网络用户都有一个基本的认知，对网络攻击有一个基本的认知，从而提升自己的防御意识和能力。其次，要强化对网络使用者的管制。为了提高网络的安全性，许多网络管理人员都会通过某种方式来控制用户的网络操作行为及权限，从而确保网络的安全性。但更多的细节，还是要靠用户自己。具体来说，个人信息安全意识的提升可以体现在如下几点：第一，设置保护口令和密码。密码是用户登录网络，正常使用网络资源的一条有效路径，因此，用户必须对密码进行保护，不能将密码泄露或丢失，以免被别人利用，从而对系统造成损害；第二，对某些机密文件进行加密，用户既是文件的创造者，又是文件的生成者，对文件具有控制权，用户要控制文件的保密程度，以及是否可以被公共访问，保证不会有非法用户进入；第三，及时地安装反病毒程序，并对其特性进行升级，使其受到的影响最小；第四，对档案进行及时的整理。多余的文件，只需要删除就行了，但与之有关的文件，还是可以保存下来的。这样会对网络安全造成一定的威胁，所以在删除的时候，尽可能使用专业的删除软件将其完全删除；第五，改善用户网的安全性。计算机网络安全技术不但包括了对计算机硬件设备的抑制和防止电磁泄漏、防盗、防自然灾害等技术，还包括数据加密、智能卡及防火墙技术等访问控制及信息保密策略设计。这就要求从业人员既要会维护计算机硬件设备，又要知道各类软件程序上的漏洞，还要筛选出未知的、潜在的安全隐患。为此，就要求从事这方面工作的人既要具有丰富的专业知识，又要具有一定的理论联系实际能力。

（二）采用信息加密技术

在网络中，信息加密是一种非常有效的信息保护手段。利用信息加密技术，实现了对重要数据、文件等的保密。信息加密技术的基本原理就是采用某种密码算法，在保证信息安全的同时，还能保证信息的完整性，利用密码技术把明文转化为无法直接读懂的秘密文本，这一技术不但适用于数据的传输与储存，还适用于程序的执行，防止了非法使用者对原始数据的访问与解读，密码学是一种用来保护程序运行过程中所用到的密码技术。信息密码技术是一种积极的信息安全防御手段，尤其是某些出色的密码算法，它不会对整个网络造成什么影响，可以对数据进行压缩和加密，在加密的过程中，一般都是通过软件来实现的，如果只有密码，那就很难破解了。在网络遭到攻击的时候，加密软件会自动关闭，而被加密的文件则会得到保护。对便携式计算机，可实现单机作业，在用户翻开加密文档时，系统会自动解密。如果用户打开了一个没有加密的文件，则由系统自动对其进行加密处理，这一过程不会对用户进入计算机，也不会对程序产生任何影响。这样做之后，将会强制地对档案进行自动加密，将档案限制在私人网络内的流动。

（三）及时采取杀毒与防火墙手段

网络带给我们便利，也带给我们危险。计算机病毒不仅对计算机系统的正常工作造成了严重的危害，而且对计算机中存储和传输信息的安全性造成了严重的威胁。在用户下载补丁、软件、文件的时候，这些病毒就会像影子一样，悄无声息地潜入用户的计算机中，破坏他们的应用程序，盗取他们的信息。所以要安装一个能提供即时病毒检测的软件，透过防毒软件对电脑进行检视，一旦发现就立即消除。然后是防火墙，所谓“防火墙”，就是用来保护电脑网络的一种技术手段，一般都是用来控制两个网络的，或者说，它可以用来控制进出双方的通讯。它是一种利用网络通讯监视技术，在一定程度上防止黑客侵入到某一单位的网络，从而达到保护计算机网络安全的目的。防火墙是一种由软硬件组成的系统，目前已经成为各个公司网络中实现其安全防护的重要手段。随着网络技术的不断进步，防火墙不仅要具备过滤功能，还要与其他安全技术相结合，例如 NAT、 VPN、病毒防护等，还需要从网络系统的数据链路层到应用层的全面安全，可以抵御外界的一切攻击。比如近年来，有一种新的防火墙技术诞生，它是建立在原有防火墙的基础上，但其安全性和过滤速度都要提升十倍以上。它的基本思想是给网络系统中的每个应用程序设定相应的代理链接，使得网络内外的通信不再是直接进行，而是经过服务器的筛选，之后再由代理服务器进行连接；极大地增强了系统的安全性，并完全阻止了入侵。并且，用户的安装也很容易，只要设置好防火墙的服务类型和安全等级，就可以直接使用。

（四）使用身份认证技术

从安全性和防御性的角度来看，身份验证的有效性要强于信息加密技术。身份验证是用户自己的一些信息，没有人可以伪造，当然这是在用户保护好自己的认证信息的情况下。最常用的验证方式就是验证密码，这种验证方式很容易实现，但安全性不高，很容易被人盗取，而且还会对网络造成威胁。验证生物特性的最佳方式，比如指纹，视网膜，面部识别等。其中，指纹是目前国际上使用最多、效果最好的一种身份鉴别方法，也是最具发展前景的一种生物鉴别技术。

四、结束语

随着互联网的日益普及，互联网信息的安全问题也日益引起了人们的重视。尤其是要重视网上电脑中所存在的信息安全问题，并采取相应的对策，合理运用防火墙、杀毒软件等，以增强网上信息安全，确保个人信息资料不被盗用。本文针对目前存在的问题，主要提出了提升个人安全意识、采用信息加密技术、及时采取杀毒与防火墙手段、使用身份认证技术的建议，希望借此提升计算机的网络安全，给用户提供安全的网络空间。

参考文献：

[1] 郭威涛 . 简析数据加密技术在计算机网络信息安全中的应用 [J]. 网络安全技术与应用，2020（05）：48-49.

[2] 陈晨 . 数据加密技术应用在计算机网络信息安全中的应用研究 [J]. 卫星电视与宽带多媒体，2020（13）：229-230.