计算机网络安全漏洞及其防范对策研究

王 新

（长春医学高等专科学校，吉林 长春 130031）

摘要：随着计算机网络的迅速发展，网络的安全问题也越来越受到人们的重视，其中网络安全漏洞包括网络系统的破坏和信息的泄漏等等，对人们的生产生活产生了非常不利的影响。因此，如何防范计算机网络安全漏洞成为当前计算机界研究的一个重要课题。本文从计算机网络安全漏洞的类型和对策两个角度展开探讨，讨论了预防和监视计算机网络安全漏洞的策略。

关键词：计算机网络安全；安全漏洞；防范策略

计算机网络安全问题是一个长期存在的问题，它对人们日常生产生活的有序开展具有重要影响。本文以网络安全漏洞的防范和监控为切入点，论述了应用网络安全防护技术，建立网络漏洞特征信息库，应用身份认证技术，应用病毒安全防范技术，有效的访问控制措施、数据加密和备份等措施在计算机安全防控工作方面的推动作用。

一、网络安全漏洞的含义

随着时代的发展，网络安全问题日益突出，计算机网络安全漏洞是造成网络安全问题的重要因素。

计算机网络安全漏洞是指在协议、软件、硬件的具体实现或系统安全策略上存在的缺陷，这种缺陷往往可以使攻击者在没有任何授权的情况下对系统和设备进行访问或破坏，造成非常恶劣的影响，计算机网络安全漏洞能影响到的软硬件设备十分广泛，包括支撑软件、路由器、防火墙，甚至操作系统本身。一些不法分子很容易利用这些软硬件自身存在的漏洞进行攻击，各类计算机病毒也能通过这些漏洞进行渗入和传播，造成严重的安全问题。如果计算机和网络受到了攻击，那么，计算机里的数据和信息就会受到影响。在当今社会，计算机网络技术发展迅速，计算机网络的破坏方式也呈现出多样化的特点。同时，各种破坏行为的相互结合也会在某种程度上增强外部破坏的组织性。同时，由于木马和病毒的泛滥，计算机网络的安全和维护工作变得更加困难。再者，随着移动电话和平板计算机等无线终端设备的不断涌现，人们对计算机的使用越来越个性化，这也给这些终端带来了越来越多的安全问题，从而使计算机安全问题变得更加复杂。

二、网络安全漏洞的类型

（一）IP 地址被盗

窃取 IP 地址是计算机网络安全中的一种常见问题，它是指某些不法之徒利用未经授权的网站来掩盖自己的身份，从而破坏使用者的网络资源，给使用者带来巨大的经济损失，由于 IP 地址通常拥有很高的权限，如果 IP 地址被窃取，将会对使用者的计算机造成很大的影响，不但会损害使用者的合法权益，还会危及到整个计算机网络的安全。

（二）计算机病毒

计算机病毒也是一种常见的安全漏洞，通常是通过人工编写特定程式，将其附着在程式码上，以破坏网络。计算机病毒对于载体适用度极高，一旦计算机感染病毒，病毒便会在其中继续进行自我复制，给使用者带来巨大的安全隐患。

（三）OSOS 与 Network 协议的缺陷

通常情况下，操作系统都存在着一定的先天缺陷，而操作系统的新功能的使用也会间接地造成操作系统的漏洞，这些漏洞主要分为控制混乱、操作系统陷害、输入输出非法访问以及不完全中介四种类型。由于 TCP/IP 技术往往不能识别 IP 的确切源头，且缺少内部控制机制，因此黑客往往会通过这种漏洞对网络数据进行拦截，获取 TCP 序列号，修改传送路径，进而导致用户遭受重大损失。

（四）对 Service 攻击的拒绝

所谓“拒绝服务”攻击，就是黑客首先对使用者的计算机进行攻击，使其计算机的正常服务遭到拒绝，从而使被攻击者的计算机系统无法提供相应的服务。其基本原理是向用户计算机发出大量的错误服务请求，造成用户计算机系统资源被阻塞，从而导致网络不能对用户的正常业务要求做出反应，造成对服务拒绝攻击。这个漏洞覆盖了服务、CPU、路由设备以及互联网宽带资源。

三、计算机网络安全问题的产生原因

计算机网络安全问题的成因通常可以归类为两大类：第一个类别是根据计算机自身的划分展开分类，一般可以分为：硬件、软件、操作系统方面的漏洞；第二类是按照使用者的身份来划分，一般分为两类，其一是使用者的安全意识不强，其二是人为恶意攻击。

（一）计算机网络硬件存在安全漏洞

计算机网络硬件中存在的安全漏洞是计算机网络中最常见的漏洞。电子辐射是计算机网络硬件的一种重要安全隐患，一般是计算机自身及网络所包含的电磁信息泄漏。而这一问题的存在为不法人员的非法获取提供了方便，也为计算机使用者带来了严重的泄密风险。另外，U 盘等移动媒体也有可能产生信息泄露问题，如果将 U 盘借给别人，那么 U 盘中的信息很可能会泄露。

（二）计算机网络软体存在的安全问题

计算机网络安全漏洞也包括计算机网络软体安全漏洞。软件漏洞经常被视为可进行恶意破坏的弱点。有关资料表明，在计算机网络安全漏洞中，计算机软体漏洞超过一半，若不能及时修补计算机网络软体的安全漏洞，将会导致计算机软体遭到攻击。计算机网络软体之安全性问题，往往被视为网络安全问题之源头，尤其是当某些使用者获得机密信息后，会产生相当数量的网络诈骗事件。

（三）计算机网络操作系统存在安全漏洞

由于计算机网络自身具备资源分享与互动的特性，因此，要想让计算机网络更好地满足使用者的需要，就需要扩充计算机网络的扩展度，以发展出更多新的应用程式，而这必然会造成网络的安全性问题。一般来说，当一个计算机的网络使用的时间越长，它的安全缺陷就会被发现。链路是计算机网络的基础，它在处理各种网络文件的时候，必然会受到文件和系统中的安全威胁。比如物理安全，协议安全，等等。这些安全隐患都可能导致信息资源丢失，进而导致系统瘫痪。

（四）用户对网络安全的认识不足

用户对计算机网络的安全性认识不足是目前威胁计算机网络安全的一个问题，用户因使用不当而造成账号资料泄露等导致计算机被攻击。由于对计算机安全意识不高，因此对计算机的安全问题并不十分重视。另外，由于用户缺乏有关的技术规范来进行网络信息系统的管理，因此很难实现对网络的监控和维护。

（五）恶意攻击

恶意攻击是当前造成计算机网络安全问题的一个主要因素。通常人为恶意攻击分为主动和被动两种。主动的人为恶意攻击一般是对计算机信号进行损害，而被动的人为恶意的攻击是对计算机的重要数据进行偷盗。人为恶意入侵往往会导致资料的泄露，从而导致信息资源的损坏或者丢失。人为恶意入侵的主要目的是盗用计算机的有关资料，而利用远程手段进行计算机操作，很容易受到诸如黑客等人为形式的恶意攻击。另外，病毒的泛滥也会严重地威胁到计算机网络的安全性。因而，病毒是人们在计算机网络上进行安全监控的一项重要内容。

四、计算机网络的安全监控与对策

随着人类的进步，计算机网络的规模越来越大，越来越复杂。要想进一步提升计算机网络的安全性，必须先对计算机网络的安全性进行详尽的认识，才能更好地掌握网络的安全性。

（一）防火墙和防毒墙的使用

防火墙一般在计算机网络中的内外部以及任意两个网络结点间设置，而防火墙的设定一般都是以重新定位的方式来识别进入的资料，并依据资料的安全性而做出允许或拒绝操作。建立一道防火墙可以对计算机的网络业务和存取进程进行即时监测，保证了对计算机的内部网的正常运行。通常来说，防火墙设置在网络入口，这与它的性能特性密不可分，因为防火墙的作用是在局域网和互联网的交接中发现和筛选病毒、非法入侵。特别需要指出的是，防火墙一般都是通过对网络入口的数据进行扫描来完成杀毒的。另外，防火墙不但可以完成对计算机的内部网络的防护，还可以在某种意义上影响到与之连接的其他网络的信息传送。由于其具有开启与关闭两种状态，所以它更像一道大门，因此，防火墙很难对计算机进行实时监控，而设立防毒墙，就是要有效地防止这种情况发生。当前，“防毒墙”已经发展成了防止和监视计算机网络安全的主要方法，许多学者都将其作为“防毒墙”的研究对象。

（二）构建基于网络缺陷的特性数据库

为了保证网络中信息和数据的安全性，必须保证计算机网络安全漏洞的精确度。建立一个完善的计算机网络安全漏洞资料库，一般要达到下列几点要求：其一，将已出现的计算机网络安全漏洞的特征及类型等信息按照特定的原则进行编码，而对计算机网络安全漏洞进行检测的过程主要是应用数据包的检测过程，所以，在进行计算机网络安全漏洞的特征及类型的相关信息检测过程中，一定要确保数据包的检测过程的准确性及高效性。其二，由于计算机网络中存在不同类型的安全缺陷，因此，正确的特性代码对网络安全弱点进行有效的解析与抽取。所以，在研究计算机网络的安全性缺陷时，必须重视其精确度。其三，借助对计算机网络安全漏洞进行特征编码的过程来扫描网络中的安全漏洞，之后借助计算机网络安全漏洞特征编码的对比过程，来对计算机网络中是否存在安全漏洞做出合理判断，并且对该信息库进行及时性的、定期性的维护。

（三）使用身份验证技术

用户的身份验证是增强计算机的安全性和监控能力的重要方法，能够有效阻止黑客的攻击。在计算机网络中，身份验证技术是保证网络安全性的关键，以此来杜绝不法分子的非法利用。计算机网络系统中的身份认证技术对维护计算机网络的安全起着至关重要的作用。计算机网络中的身份认证过程主要包括使用者的身份认证及使用者身份识别链这两个方面。通过对身份认证技术进行合理应用，可以将使用者的物理身份及数据身份进行对比，确保使用者使用计算机网络权限的安全性。值得注意的是，在借助身份认证技术对使用者的身份进行认证时，要将使用者使用身份是否合法的验证过程作为该过程中的首要内容，以此来杜绝不法分子的非法冒充，维护使用者的信息安全，确保整个计算机网络系统的正常运行。对该技术进行应用的计算机网络中的使用者的数据身份，不仅能在一定程度上控制使用者的使用计算机网络的权限，同时也会影响整个计算机网络的安全性。

（四）安全和预防病毒技术

计算机病毒善于攻击计算机网络中的弱点。另外，当计算机病毒侵入计算机时，它会根据自己的依赖性和多样性，很快地找到计算机的弱点从而达到对它进行攻击的目的。为了增强计算机系统的安全防护性能，需要对具体的攻击目标进行研究。首先，我们在计算机上安装杀毒软件，利用这个杀毒软件来抵御入侵病毒的入侵。同时，我们也要对计算机进行定期的检测，以保证计算机的安全性和完整性。接下来就是建立一个新的杀毒系统了。计算机病毒的变异并不是一成不变的，而是可以大规模复制的，而且这些分体通常会具有比原病毒更强的程序性及操作性。所以，有关人员必须做好对计算机病毒库的更新，以最大限度地利用病毒库防止各种病毒入侵。之后是阻止病毒的侵入，防止恶意插件侵入计算机系统，为计算机搭建一个安全的使用环境，最大限度地保障计算机的安全。

（五）有效的访问控制措施

对计算机的访问进行监控，其方法有：身份验证和访问控制网关。访问管理网关设置在网络的入口处和边缘，在计算机网络中设置一个身份验证服务系统从而达到对计算机网络系统的保护目的。在计算机网络中建立访问管理机制能够对有关的数据进行检测和筛选，从而保证授权控制有效实现，同时也可以验证用户身份。

（六）加密和备份资料

在计算机网络中，对信息进行加密是保护信息安全的一种有效方法，而加密算法是其中的关键技术。加密算法主要分为三种：不可逆的加密算法、对称性的加密算法、非对称性的加密算法。在计算机网络系统中，对数据进行加密是为了保证数据的安全性。但是一些人为因素、自然灾害等因素，也会对网络安全造成一定的影响，因此，我们需要做好数据备份工作。备份的方法包括备份、硬件备份和软件备份。

五、结语

计算机网络的迅速发展，为人们的日常工作生活提供了便利，但也带来了一定的信息安全隐患。为了更好地利用计算机网络的优势，防范计算机安全隐患，我们必须对其进行有效的研究。计算机网络的安全性和脆弱性是一种普遍现象。值得注意的是，计算机网络的安全与漏洞是两个共同存在的事物。因此，相关研究者一定要有针对性地看待计算机网络安全漏洞问题，并采取恰当的措施来进行防范与管窥，来确保计算机网络的安全性。

参考文献：

[1] 邱寒 . 计算机网络安全的漏洞及防范对策探究 [J]. 电子世界，2021（08）：21-22.

[2] 王铮 . 计算机网络安全漏洞分析及防范对策探讨 [J]. 电脑知识与技术，2020，16（29）：55-56.

[3] 卢俊睿 . 计算机网络安全漏洞及防范策略分析 [J]. 中国新通信，2020，22（08）：88.

[4] 颜清华 . 信息化背景下网络安全漏洞与防范措施分析 [J]. 信息与电脑（理论版），2019（12）：217-218.