计算机通信网络的安全与防护技术

张红磊
天津卓朗科技发展有限公司　天津　300400

摘　要：计算机网络通信安全问题是一个需要重视的课题，否则轻则干扰电脑的运行，重则造成电脑崩溃，特别是巨大的数据资料的外泄造成的损失不堪设想。所以为了加强计算机网络通信安全管理工作，需要对其面临的安全问题加以研究，从而制定针对性的保护措施，能够有效地促进计算系统安全有效的工作。

关键词：计算机；通信；网络安全；防护策略

引言

电脑通信安全问题是一个需要重视的问题，不然轻则影响电脑的应用，重则造成电脑崩溃，特别是巨大的数据信息的泄露造成的影响不堪设想。所以要加强计算机网络通信安全管理工作，需要对其面临的安全问题加以分析，从而制定针对性的保护措施，才能更好地促进计算安全高效地运行。

1 计算机通信技术概述

对电子计算机数据通信技术进行的研究表明，它是一门以数据通信方式为基础，通过对电子计算机的终端设备在电子计算机与计算机之间相互传递信息并进行服务的信息技术活动，是现代通讯技术与计算机科学密切结合的结果。以传输的方式为基础，可以把电脑通讯方式区分为直接电脑通讯和间接电脑通讯，其中，前者指由二台或几台电脑直接连线完成的通讯，相应的通讯形式涵盖了点对点和多点同播，而后者则主要指通讯方式基于交换互联网进行的传输方式[1]。

2 计算机通信网络安全内涵

对计算机通信网络的数据分析可知，其中最重要的数据是基于网络的大量数据，这些资料不但包含了网络使用者自己的个人资料以及上传的全部信息，同时也涵盖了各大网络运营商所开发的各种业务能力，从这一角度出发，计算机网络通信安全则不仅只涉及网络的安全性，同时还涉及了以网络为基础的各种信息系统的安全性。所以，在建立计算机通信网络的过程中，除从多方面掌握计算机通信网络建设之外，还应以通信信息的具体特征为基础建立出具体的安全策略，从总体上保证了计算机通信网络的安全与可靠性[2]。

3 计算机通信网络安全的特点

计算机信息技术导致网络安全产生多样性、复杂性、系统性的特征。要确保互联网平台安全，最关键的手段就是要具备一定的防范措施，也需要进一步改进和加强安全制度。在安全隐患的表现形式和内涵中必然存在着多元化，这是由于网络安全的多元化，需要对其有效应对，因此需要进一步完善和提高网络的安全技术[1]。网络的安全体系要求信息技术和网络系统的体系化，需要完善网络安全制度，并建立完善的安全体系，使计算机与通信等网络系统在复杂的运行环境中平稳地安全工作。要对计算机通信及网络系统的有关安全防范措施加以合理改进和优化，对安全问题有很大影响。如今采取了客户端上网模式，这样通信网络系统不再独立，变得复杂多变，相关的对网络安全产生威胁的各种因素将随之增多。网络各方面均对计算机系统安全有威胁，但是，网络技术的进展，计算机通讯安全方面必须继续努力与改善，从而确保在网络环境中的通讯网络能够安全工作[3]。

4 计算机通信网络的安全防护意义

在计算机设备的信息传输中，往往命令操控点都是在应用终端上，用户完成网络申请后，可以进行搜索网络资源库，使用户的信息资源能够有效连接于网络资源[2]。其所形成的数据交换网络，可以实现在广域网、局域网的要求下，让通讯机制实现有效信号传递的目标，实现使用者与设备进行有效通讯。从信息传输的视角分析可以得出，信息载体与通讯网络之间的定向化信息传递关系，可被看成一个有机整体，通过有机融合传输、储存和管理，真正实现了对接大数据信息的目标。

5 算机通信网络常见的安全问题

5.1 系统软件的泄露

因为应用软件开发商在设计应用软件中，不能根据用户的各种要求加以合理实现，就不能把应用软件实现非常完善，软件在使用中就出现相应的缺陷和缺点[4]。而也恰恰因为这种缺陷和不足，被一些不法分子抓住可趁之机，往往通过这种漏洞实施一些违法犯罪活动，对使用者的有关资料信息实施盗窃，从而给使用者的国家权

益带来很大损失。

5.2 计算机病毒

木马病毒和计算机病毒都是电脑上比较严重的问题，这二个病毒通常发生在计算机程序上，对计算机程序加以攻击，进而执行恶意的命令，从而导致计算机信息的泄漏，在更严重的情况下还可能对电脑的硬件产生冲击。这种病毒可以提供很有效的伪装，而且还可以实现自我拷贝，所以如果电脑上遇到了这种病毒感染，就很难对病毒加以处理，但这种病毒也拥有良好的传播速度，从而可以带来更多的危害。

5.3 黑客的攻击

在算机通信网络中黑客的攻击是安全威胁中最为可怕的一种。当用户的计算机出现黑客攻击后，就会在网络运行正常的情况下，进行攻击行为，对计算机中的相关信息进行获取。黑客攻击的危害性较高，也会造成用户较大的经济损失[5]。

5.4 用户方面

许多计算机用户不是专门技术人员，但是在应用过程中常常因为安全意识的欠缺而产生人为的安全问题。例如不设定开机密码，设定的密码非常简单，但运行中没有对其的防护，浏览不法网址、钓鱼网页，造成电脑数据信息被盗取或者修改。给病毒和木马的入侵带来了可乘之机，所以，此类问题应该受到人们的关注。

5.5 安全意识较为淡薄

很多用户在使用计算机过程中缺失网络安全意识，这也会给某些犯罪份子可供可趁之机。用户在安全配置中没有安全措施，密码设定不够简单等也会存在很多安全隐患。同时不少人在使用网络过程中，对一些来历不明的网页进行浏览，这都可能产生安全隐患，给客户的网络安全和资产安全性带来很大冲击。客户安全意识的薄弱已经是互联网隐患的比较明显的现象，所以客户应进一步增强自己的安全意识，减少发生网络安全事故的风险[1]。

5.6 计算机网络自身方面

因为个人电脑在连接环境中具备了较好的适用性，所以能够连通宽带上网、无线网络、局域网网络、3G/4G网络等，并具备了较好的开放性，但不同的局域网类型所面临的安全风险又有所不同，尤其是较为普遍的宽带互联网的使用，由于布线十分复杂，实际应用也较多，所以在传递大数据信息时往往在安全和保密性上都无法适应人们的实际需求。由于有的电脑本身存在缺陷，特别是缺陷修补不到位、程序出现缺陷时，常常成为骇客和不法分子的攻击目标。

6 计算机通信网络安全防护的相关方法

6.1 数据加密技术的应用

数据加密技术，指数据传送方通过加密密钥和加密函数对信息明文进行加密，使之转化为无价值的数据秘密文件，而数据接收方通过解密密钥和解码函数对附加的密文进行解码，并将之转化为数据明文的方法[2]。数据加密技术是当前数据加密技术是当前保证计算机数据传输安全的核心技术。以链路加密与节点加密为例，对这一方法的使用原理加以阐述。链路加密对计算机或通讯网络中的所有信息进行加密的基本原理是，先在消息传输方发送信息之前对所有信息进行加密处理，当消息在各节点的传送过程中被破译后，再继续使用下一条链路密钥加密相应节点的消息，之后，再将消息传输至信息接受方。数据通信网络的链接加密使得对信息的源头与终端都进行了较好地覆盖，也因此有效增强了计算机与数据通信网络系统的稳定性。节点加密是指利用与节点机连接的密码设备实现信息加密和解密的通信安全技术手段，与链路密码技术类似，它也会在计算机传输链路内为所有需要传输的信息，提供对信息源点和终端的安全保护，而节点加密技术则在对信息加密时，不允许将信息以明文形式在各节点间显露出来，因此，更加增强了整个计算机通信网络系统的安全。

6.2 身份识别技术的应用

身份辨识技术也是当前中国计算机网络通信安全保护使用的另一种主要技术手段，该技术主要分为基于口令的身份识别和基标记的身份识别二类，其中，基于口令的身份识别采用设置长度为5-8、由数字与字母所组成的字符串，来形成对使用者身份的认证;而基于标识的身份识别则以个人持有物作为识别基础，当该计算机开启时，电脑将通过对系统里面含有的信息加以鉴别而完成身份验证[3]。一般情况下，身份的方式大都以基于口令的身份出现，信息传递的查询者在进入计算机系统之前，首先进行用户的身份认证，在认证通过之后，才可以在相关的系统当中完成数据的查询与传递。身份标识因其快捷、有效的安全性优势被应用于电脑通讯系统的安全保护中，进而导致非法客户难以随时查询当前的系统数据，有效增强了电脑通讯系统的安全。

6.3 优化计算机通信系统

对计算机进行改装可以有效提高电脑通讯网络的安全性。由于对的电脑通讯网络系统设计相对比较简单，出现不少漏洞，这将导致安全问题的产生。因此技术人员必须要提高自己的技术，通过对目前的系统技术有效的改进和提升，可以科学合理的减少软件系统中出现的

安全问题。同时也要积极完善安全检查机制，技术人员也要有计划的对软件系统实施检测，这样就可以及时发现应用软件系统中出现的问题，并及时加以处理。

6.4 防火墙的应用

边界防火墙的运用，即在内部网络联入Internet时，为了保证内网安全性，在内网与Internet之间建立了一个中介网络，对来自外界互联网上的安全风险进行隔离，从而构成了对内部通信网络的防护体系;

分布式防火墙的运用，即通过对内部合法链接的安全策略进行集中定义，或由部分节点单独执行这一安全策略，对每个结点，都有与其相应的认证，如同该结点的公钥相对应数字证书，在这个环境下，网络管理员也就能够和本地的系统管理员同处一人，又可同本地网络经营者不同，因此网络经营者可以通过自己所拥有的数字证书来确认自身地位，从而对已有的网络拓扑技术的限制进行打破，由此可以增强计算机通信网络的安全保护作用[4]。

6.5 入侵检测技术

防火墙可以保证内部网络系统不受到外界网站的入侵，但是它对内部网站的一些非法活动的监测还没有完善。作为对防火墙技术的合理补充，IDS(入侵检测系统)积极主动的措施实现了系统对内部入侵、外来攻击和误操作等的信息防护，在系统遭受侵害之前截获信息并应对攻击，从而增强了安全性。该技术通过监测受保护操作系统的状况与行为，通过异常侦测及误用分析的手段，识别未经许可或非法的操作系统和互联网活动，为防止攻击活动的有力措施。

6.6 完善计算机通信网络系统

安全是计算机通信系统中最为关键的因素，因此在系统设计中一定要将系统安全作为基础。系统设计人员在设计过程中，要架起那个对国内外先进技术的研究与学习，不断克服系统设计中遇到的阻碍，同时也要将系统的缺席进行合理弥补，提升系统的安全。系统设计人员要对通信网络安全技术进行合理探究与应用，可以让专业的技术人员对通信网络安全技术进行讲解，积极组建研究小组，加强新技术的研发，这样才能为用户提供更加安全稳定的网络环境[5]。同时我国也要加强对计算机通信网络系统的研发投入，优化研发环境，保证设计人员能够不断创新思维与技术，为人们提供更加安全与稳定的计算机通信网络系统。

6.7 漏洞扫描技术

漏洞扫描技术也是一种主要的安全方式。它与防火墙、攻击侦测技术互相配合，可以有效增强互联网的安全。通过对互联网的扫描，互联网管理员可以知道互联网的安全配置以及运行的应用服务，及时发现安全漏洞，客观判断网络安全危害程度。网络管理员也可通过数字化扫描的技术更正网络安全漏洞以及操作系统中的出错设置，在黑客攻击时做好预防。而如果防火墙等网络安全监视系统只是被动的防护措施，那么安全数字化扫描技术便是一个积极的预防措施，可以有效防止黑客攻击行为，从而做到防患于未然。

6.8 访问控制技术

在网路系统管理中，基本上任何一种计算机都有基本的对访问身份权限的管理的。如果计算机具有合理的设置，并且如果系统内的对文件的存取权限能够加以适当的设定，那么访问控制就能够对于访问者的存取加以适当的限制，对超过其权限范围的存取也就能够进行避免。不过访问控制也是具有一定的漏洞的，因为它并没有对任何访问加以管理，但是只要某些人对计算机系统的漏洞加以使用，这些访问者就能够得到与用户相同的访问权限，所以尽管这只是一个网络攻击，不过对访问控制而言却是一种完全正常的使用。

结语

电脑通信安全问题是一个需要重视的课题，不然轻则干扰电脑的应用，重则造成电脑崩溃，特别是重大的数据资料的泄露造成的损失不堪设想。所以要加强网络通信安全管理工作，需要对其面临的安全问题加以研究，从而制定针对性的政策，可以更好地促进计算系统安全有效地工作。

参考文献

[1]黄磊.新形势下计算机通信网络安全隐患及其对策探讨[J].中国新通信，2020，22（05）：30.

[2]袁捷.新形势下计算机通信网络安全隐患及对策探讨[J].技术与市场，2019，26（05）：219.

[3]王祥.新形势下计算机通信网络安全隐患及其对策探讨[J].通讯世界，2019，26（04）：157-158.

[4]张国宸.新形势下计算机通信网络安全隐患及其对策探讨[J].通讯世界，2019，26（02）：79-80.

[5]冯静.浅析计算机通信网络安全与防护[J].数字化用户，2019，025（002）：134，262.