通信工程网络安全与对策探讨

陈涛

（浙江省公众信息产业有限公司，浙江　杭州　311100）

摘　要：信息化发展进程中，社会群众开始关注网络安全问题，需要通过网络安全体系，维护银行信息、个人信息。在信息时代发展中，网络安全协议关注度持续提升，可营造安全网络环境，属于互联网技术重要因素。网络安全协议能维护互联网安全，避免泄漏网络用户信息，保障网络数据传输安全性，有效作用于计算机通讯技术中。

关键词：通信工程；网络安全；网络信息

1　通信工程网络安全问题分析

1.1　网络信息盗取问题

目前很多计算机用户在使用通信工程网络系统的过程中，安装部署、管理模式非常简单，虽然能够简化操作流程，但是很容易出现通信网络的安全隐患问题，不能全面进行通信网络的安全防护，很容易在僵化的安全管理方面出现信息泄露的现象。尤其是在适应第三方软件的过程中，可能会因为软件存在漏洞问题，所使用的安全保障措施也不到位，或者是和网络系统本身的安全机制存在冲突，导致木马病毒进入到系统内部，出现干扰的问题，非法获取到网络中的信息和资料，对整体网络信息的安全性产生威胁。

1.2　网络本身存在潜在隐患

通信工程中的网络安全问题发生的主要原因，就是网络本身存有潜在的隐患，由于因特网中所采用的协议是TPC/IP，优势在于实用性较强，但是劣势就是安全性很低，潜在隐患问题较多，例如：在电子邮件的服务方面，是将因特网协议当做是基础部分，设备很容易受到病毒的入侵或者是黑客的攻击，风险问题的发生率较高，安全问题出现的概率很大[1]。

1.3　内外网的安全问题

通信工程领域中会涉及到内外网，合理进行内部和外部网络的隔离处理、连接安全性管理非常重要。但是目前部分通信工程中的内部网络与外部网络方面还存在隔离问题，不能合理设置隔离的系统与连接安全管理系统，经常会导致内部与外部网络连接期间出现信息安全隐患问题，对整体系统运行的安全性造成不利影响。

1.4　安全技术应用的问题

虽然目前在网络安全管理的工作领域中已经开始应用防火墙技术、入侵检测技术、病毒查杀技术等等，起到了良好的成效，但是，在技术应用的过程中还存有很多的安全隐患，不能结合通信工程网络系统的实际运行情况针对性的使用安全技术措施，严重的还会引发信息泄露问题、系统入侵问题等等，威胁着通信工程网络的运行安全性和可靠性，对其长远进步和发展产生非常不良的影响。

2　通信工程中网络安全问题的对策

2.1　预防出现信息盗取的问题

为有效预防通信工程中出现网络信息盗取的安全问题，应强化内网的通信安全管理力度，确保内网通信的安全性，维护整体通信系统的运行效果。

2.1.1　应积极使用安全交换机系统

主要因为网络信息传播的过程中，会使用广播技术，可能会在广播域中出现数据包被监听或是被截取的现象，所以应该按照实际情况应用安全交换机，通过网络酚酸方式、VLAN方式等，从物理层面或是逻辑层面进行网络资源的隔离，确保内网的安全性符合标准。

2.1.2　严格进行操作系统的安全管理

无论是操作系统中的终端用户程序还是网络技术，都必须要合理使用安全的管理方式，在操作系统中设置安全补丁，开展相应的监控工作，制定用户口令制度和访问控制制度，在维护通信网络安全性的情况下，可以更好地执行管理任务。

2.1.3　应该积极采用代理网关

将其应用在网络安全管理的工作领域中，能够确保数据包交换的安全性，不会直接在内网区域中执行，内部的计算机系统也可以利用代理网关才可以进行因特网的访问，这样不仅可以提升操作的安全性，还能保证代理服务器应用期间，全面限制网络内部访问，保证信息的安全性，不会出现被盗取的现象[2]。

2.1.4　重点应用密钥管理方式

主要因为目前很多通讯工程网络入侵者，都是先进行用户口令的破译，然后入侵到网络系统中，或者是寻找网络系统中薄弱部分、漏洞部分入侵，对网络的安全性产生破坏性影响。在此情况下就应该重视在内网的平台和系统中设置密钥，开展密码管理的工作，在设置密钥口令期间需要注意，尽可能增加口令的位数，不可以选择显而易见的密码当做是口令，也不可以在不同系统中使用同样一个口令，在无人的状况下输入口令，同时还需定期进行口令的更改，利用破译口令程序进行文件安全性的监测，保证信息不会被盗取。

2.2　严格控制网络本身的安全性

为了确保网络自身的安全性，在工作中应该严格开展网络信息传播的安全管理工作，以免在通信工程网络信息传播期间发生安全隐患问题，从根本上增强整体的网络信息安全性。

2.2.1　积极使用数字签名技术

利用加密算法形成符号或者是代码所组合而成的电子密码签名，替代书写签名或者是印章，此类电子签名验证的准确性较高，可以通过验证明确文件传输期间有无改变，保证文件信息的完整性与真实性。采用数字签名技术，还能预防出现信息人为修改的现象，增强所有数据信息的机密性，完善其中的身份识别功能，并且不具有一定的依赖性，在一定程度上还能够加快交易的速度，保证交易的准确性。

2.2.2　应用数字集群系统的安全技术

对于数据集群系统来讲，其中的信息安全会涉及到用户鉴权方面、加密方面、分级管理方面、虚拟专网方面、日志管

理方面，可以将系统划分成为专网、共网两种运营模式，无论哪种模式，都对通信的覆盖率提出很高的要求。一般情况下，数字集群通信系统主要使用在应急通信方面，业务量具备较高的突发性，为保证安全性，应该做好拥塞的控制工作，同时根据系统的运行特点、安全问题发生规律等，采用针对性的方式和手段规避预防安全隐患问题，从根本上维护整体系统运行的安全性。

2.2.3 合理使用量子密码加密技术

主要是将密码学技术和量子力学技术相互结合，将量子状态当做是信息加密的密码、解密的密钥，为提升通信工程网络信息安全性提供一定的保障。首先，应该将单光子量子通道之内的海森堡测不准的原理当做是主要部分，确保所制定信息安全方案符合要求。其次，应该将非正交量子态性质当作是基础部分，合理制定相关的方案，深入研究其中的量子密码内容，明确是否已经逐步分发量子密钥，创建有关的密钥系统，保证技术的应用效果，维护所有数据信息的安全性[3]。

2.3 积极采用先进的隔离技术措施

为保证通信工程中的网络安全性，还应该整合各种不同的系统，采用隔离技术维护网络安全性，利用外端的客户端，实现内部与外部网线的交换处理，解决目前存在的安全问题，在隔离技术的支持下、监控技术的帮助下，确保内外网之间的安全性。首先，对于用户所使用的计算机服务器来讲，提出申请的过程中必须要做好程序的认证工作，如果与之前所登录的服务器存在不同之处，就必须要拒绝网络的接入，不允许网络端口的开放，如若用户已经进入到相关的区域，就必须要在服务器登录期间提出有关的预警信息。其次，具体的服务器数据库记录操作期间，需要执行用户访问的排序处理工作，定时进行服务器数据信息的内外网互换，将存储的序列发送到另外一个服务器，同时进行标记处理，如果用户存在违规操作的现象，就不可以与外网之间相连接。最后，应该准确记录用户登录服务器的具体时间，开展相应的监控工作，于客户端中使用安全系统，保证服务器联网期间正常并且合法的使用。还需注意，如果用户关闭了有关的安全系统，不能正常接收序列信息，就必须要开展安全系统的处理工作。

2.4 积极采用基本性的安全技术

通信工程领域中为了维护网络安全性，应该积极采用基本性的安全技术，发挥技术在维护网络安全性和稳定性方面的作用优势，不断增强通信网络数据信息的完整性，预防出现泄密现象、系统被篡改现象、系统被攻击的现象。首先，应重视防火墙技术的应用，在网络之间形成屏障，预防出现信息资源的非法入侵现象，保证所有数据信息的良好互动交流。其次，应重点应用先进的数字签名技术，就是在网络系统中实现算法加密处理，生成有关的代码，不再使用传统的签名形式，可以及时了解到电子文件在传输期间是否有更改或是盗取的现象。最后，采用入侵检测技术，通过入侵检测系统实时性、动态性的检测网络是否存在入侵的风险问题，一旦检测到有入侵风险，就可以立即进行处理，如果不能自动化的处理，会向技术人员发送预警信息，技术人员可以按照预警信息合理进行修复处理，保证网络系统的安全性[4]。

3 结论

目前在通信工程的网络系统运行和发展的过程中，受到很多原因的影响，经常会发生安全隐患问题，不利于维护网络的安全性。所以在新时期的环境中应重视通信工程网络安全管理，合理使用先进的安全管理技术措施，按照安全问题的发生特点、规律与实际情况，深入性的开展有关安全管理和维护工作，从根本上增强整体网络的安全运行效果。

参考文献

[1] 包卫东 . 通信工程网络安全与对策讨论 [J]. 中外企业家 ,2020,33(1):251–266.

[2] 刘俊鹏 . 通信工程网络安全与对策讨论 [J]. 建筑工程技术与设计 ,2020,13(7):59–67.

[3] 李军鹏 . 计算机通信网络安全与防护对策探析 [J]. 建筑工程技术与设计 ,2018,22(15):48–67.

[4] 薛力瑞 . 计算机网络工程安全问题与解决对策探析 [J]. 中国新通信 ,2020,22(9):151–166.