通信工程网络安全问题与对策分析

费秀晶　杨晓玲

（重庆首讯科技股份有限公司　重庆　400060）

[摘　要]在科学技术高速发展的现如今，我国已正式步入新信息时代，通信工程的重要地位逐渐凸显。在此背景之下，通信工程的网络安全问题备受关注，成为影响其长足发展有效应用的重要因素，增强网络安全尤为必要。基于此，现结合实际情况对通信工程的网络安全问题进行深入分析，并提出相应的解决措施，以推动通信工程的健康有序发展。

[关键词]通信工程；网络安全；信息时代

【DOI】10.12252/j.issn.2096-6288.2021.06.2474

引言：

通信工程又被称为电信工程或信息工程，是融合有线通信、无线通信以及电子技术专业，以通信过程中信息的传输以及信号的处理与应用为落脚点的综合信息工程。通信工程的衍生与发展成为推动社会发展与改善人民生活的原动力。但是由于技术发展的局限性，通信工程面临严峻的网络安全问题，信息盗取与泄漏问题层出不穷，对于社会各个层面的信息安全及经济发展造成威胁，不利于社会经济的稳定发展。基于此，深入分析通信工程的所存在的网络安全问题，制定完善的应对机制，提升通信工程的稳定性与安全性，实现价值最大化。

1通信工程网络安全存在的问题

通信工程的信息传输依赖于计算机外网技术，而信息的处理依赖于信息内网处理技术，而威胁通信工程网络安全的主要问题源自于以上两个基本技术环节。具体而言，其问题主要集中于以下方面。第一，从计算机网络技术视角而言，现行的因特网的所采用的协议具有实用性较强的优势，但是安全性能明显不足，防火墙的设计存在明显的局限性，无法保证计算机网络的绝对安全，导致病毒与黑客入侵问题屡见不鲜，不仅威胁网络的安全性，而且极易造成计算机工程的损坏。此外，一些计算机用户的网络安全意识较为薄弱，为了简化操作流程而采取较为简单的管理模式，为木马病毒的侵入创造了有利条件，造成信息泄漏的威胁。第二，从通信工程网络信息技术视角而言，内外网的隔离措施不到位，内外网的衔接成为薄弱环节，存在较大的信息安全隐患，影响系统的整体运行的稳定性。此外，安全技术的应用的针对性较为欠缺，尚未满足现阶段的网络系统的实际运行需求，对于系统入侵、信息泄漏等问题并未采取行之有效的安全应对策略，对于不明访问权的控制力度不足，防火墙并未真正实现其应有的安全维护价值，难以抵御恶意攻击。综上所述，加强通信工程网络安全建设极具必要性与紧迫性。

2通信工程维护网络安全的措施

2.1加强安全管理，提升内网防御

内网技术作为通信工程发展的重要载体加强安全管理，提升内网通信的稳定性与安全性是保证通信系统有效运行的重要手段。第一，注重安全交换机系统的高效运用。广播技术是网络信息传播的重要媒介，而在此过程中极易出现被监听或拦截等问题。针对此情况运用网络酚酸或是VLAN方式等安全交换机实现网络资源的隔离，保证内网安全性。第二，规范操作系统运行。根据实际情况，在操作系统中设置安全补丁，以实施全方位的安全监控，针对用户口令及访问控制实施严谨规范的制度管理，以减少因操作不当而造成的安全隐患。第三，强化代理网关。通过设置代理网关使数据包交换不会在内网区域中直接执行，增设内部计算机系统的网络屏障，在保证网络安全的同时，能够在代理服务器应用期间实现网络内部访问的全面限制。第四，应用密钥管理方式。针对通信工程网络入侵大多是先进行用户口令的破译，再对网络系统的薄弱环节进行攻击的情况，在内网平台设置严谨的密钥管理屏障，采用较为复杂的密钥口令，定期进行更改轮换，为内网平台增设一层防护罩有效打击，通过破译口令攻击网络安全的行为。通过加强内网信息技术建设，提升防护能力，有效预防不良行为的侵袭。

2.2弥补薄弱环节，增强外网安全

互联网技术本身的漏洞是通信工程网络安全所面临的较为严峻的挑战。针对此情况，在网络信息传播环节实施强而有力的安全管理，将互联网本身的安全问题降到最低。具体而言，尝试从以下方面着手。第一，运用数字签名技术。传统的手写签名或是印章安全系数较低，极易被破译。针对此情况，采取加密算法形成的符号，又或是代码所组成的电子密码签名等更为精密的数字签名技术，提升验证准确性，能够察觉文件传输过程中细微的变化，以增强文件信息在流通过程中的安全性与真实性。此外，借助数字签名技术增强信息的机密性，强化身份识别功能，有效杜绝篡改信息等不良行为。第二，构建数字集群系统。信息安全涉及用户鉴定权、加密、分级管理、日志管理以及虚拟专网等多个层面。因此，数字集群系统的构建需要从共性及个性需求两个视角进行考虑，采取公网与专网的双重运营模式。数字集群系统对于通信覆盖率有着较高的要求，在具体实践过程中应积极落实拥塞控制管理机制，以保证其安全维护互功能的充分发挥。此外，深刻掌握系统的运行特点，洞察安全问题发生规律，对于非一般情况的网络安全问题实施特事特办，采取针对性的防御手段。通过对外网技术短板采取有效的规避措施，提升网络体系的安全性。

2.3强化安全技术，构建防护体系

就目前而言，通信工程的内网与外网并未实现有效隔离是影响网络安全的又一重要因素。基于此，立足各个网络系统的个性化特征，采取相契合的隔离技术措施，构建内外网之间的保护屏障。一方面对于用户计算及服务器而言，完善认证机制，借助隔离系统能够辨别所登录服务器的异同，及时拒绝陌生服务器的接入。针对已经进入的用户则设置相应的预警信息，以随时监察其行为动向，有效规避风险。另一方面应加强用户访问排序处理工作，实现核心数据的内外网交换，形成自查系统及时发现违规操作现象，并采取相应的规避机制。并对用户登录时间进行详细的记录，实施全程性跟踪。第二，采取基本性的安全技术。基本性安全技术对于维护网络的稳定与安全具有不可取代的作用。因此，应加强通信工程网络数据信息建设，强化数据的完整性。一是完善防火墙技术，在各个网络之间形成必要的安全保障，为数据信息的互动提供有力支持。二是实施算法加密处理，增强关键数据信息的隐秘性，有效限制访问权限。三是建立健全入侵检测技术。对于进入网络的用户实施即刻性与持续性的监测，对于网络安全实现全方位的检测，对于细微的安全威胁予以立刻处理，而对于较为复杂的安全问题则向管理人员提出预警，将安全风险降到最低。

结束语：

随着通信工程的发展，逐渐渗透至社会生产与人民生活的各个领域，加强网络安全维护，既是保证通讯工程的有序发展，也是维护社会安定的有利举措。因此，各企业需要及时把控网络的发展特性，增强网络安全防范意识，不断完善网络技术，以净化网络环境，促使通信工程能够更好的服务于社会。

参考文献

[1] 张玉昭. 关于通信工程网络安全研究[J]. 建筑工程技术与设计,2021(19):1417.

[2] 张曦月. 主动防御技术在通信网络安全保障工程中的应用研究[J]. 电脑知识与技术,2020,16(4):28-29.