浅议通信工程网络安全与解决对策

刘以安
广东省电信规划设计院有限公司

[摘　要]通信工程技术已经渗透到人类生活的各个领域，并有力的推动了人类的经济发展，为社会建设节约了劳动力。以此同时，破坏信息安全性和机密性的问题也越随之增多，本文主要浅析网络通讯工程中存在的网络安全问题，并针对存在的问题提出相应的解决对策。

[关键词]通信工程；网络安全问题；解决对策
【DOI】10.12252/j.issn.2096-6288.2020.02.1777

引言

我国的通信事业正在高速向前发展，通信工程也随之快速发展，为社会的进步做出了巨大的贡献，对人类的生活产生了巨大的影响。但随着网络通信技术的进步，各种网络攻击、侵入及数据泄露层出不穷，网络及信息安全也成为亟需重要对待的问题。通信工程的网络安全问题与个人、企业、乃至国家的安全密切相连，认识通信工程网络安全存在的问题，同时细致分析导致问题存在的原因，并研究解决策略势在必行。

1 通信工程网络安全存在的问题

通信工程也称为电信工程或信息工程，是信息科学技术的一个领域，是通信过程中的信息传输和信号处理的原理和应用，是数字移动通信、光纤通信、网络通信相关技术相互渗透、互补而发展起来的综合性通信工程的处理和应用。在通信工程中，信息主要包括内部信息的处理与和外部信息的传递，即通信网络的内联网处理技术和外部网络技术。按照以上两项基础技术，提出以下几点网络安全在网络安全通信工程中的重要性。

1.1内网网络安全问题

内网是局域网，是网络通信工程在内部数据处理过程中使用的网络，内网的系统安全技术措施做不好，将导致内网系统瘫痪。内网也必须保证网络信息的可靠性、实用性、完整性和机密性的安全性，如果内网系统漏洞利用或者被病毒攻击，会造成信息泄漏或系统瘫痪，内网整体安全性能受到影响。

1.2外网网络安全问题

外部网络是广义的互联网，通过连接外部网络，可以实现全球互联，在外部网络领域可以获得大量的数据信息，人们可以根据需求从中选择有用的信息。互联网信息传播具有形式多样、信息传播及时及时、信息无限复制和传播的特点，因此，在传播信息的过程中，信息被盗用的可能性很大，安全问题包括以下：

（1）计算机网络系统设计存在问题：在进行计算机系统的设计过程中，没有形成清晰、简洁的网络布局和系统架构，没有在网络边界设置安全防范，在存在这些问题的情况下，计算机与外部网络进行交互，从而将会造成安全隐患。

（2）防火墙的局限性：防火墙的作用是避免计算机外部的恶意软件攻击计算机的内部系统，然而，在进行实际工作过程中，防火墙在一定程度上阻止了恶意软件的入侵，但并不能在最大程度上确保计算机网络系统的绝对安全，防火墙不能解决来自内部网络的攻击和安全问题，防火墙无法解决TCP/IP等协议的漏洞。

（3）安全设备配置不足：在遭受网络攻击的时候，所选产品性能不佳，处理不了网络攻击，发挥不了实际作用。

（4）病毒入侵：编译器将恶意数据程序病毒插入您的计算机，该病毒会对计算机系统的运行功能造成破坏，并将会对计算机的正常工作造成影响。该病毒具有破坏性、超寄生性、快速传染性和隐蔽性，是对计算机网络安全的一个最重要威胁。

（5）数据泄露：未授权访问，员工错误、疏忽、处置不当，黑客入侵等利用计算机的安全漏洞，获取计算机的数据和信息，对计算机的功能造成破坏。

1.3缺乏专业人才

如您所知，管理信息系统有四个基本环节：运行、管理、建设和维护，通信工程也是如此。目前通信技术急剧发展，而掌握新技术，能参与建设、管理、运行维护的人员比较缺乏。总之，专业通信工程人才的缺乏会大大降低通信系统的日常专业维护成果，使通信系统在紧急情况下的快速修复更加困难。因此，为了在最大程度上提高中国通信系统的工作效率和安全运行稳定性，有必要不断提高通信工程团队的专业素质和业务素质。

1.4硬件设备安全隐患

在信息通信网络运行期间，硬件设备的损坏会对网络系统整体运行的可靠性和安全性造成直接影响，在当前信息通信网络系统建设过程中，软件系统通过虚拟“云技术”运行，硬件设备成为重大安全隐患。在进行硬件设备建设期间，需要对建设方案进行详细分析，确保通信系统硬件设备建设的可行性，在最大程度上降低硬件设备与居民日常生活发生冲突的几率。

2 解决通信工程中的网络安全问题

信息安全包括十分关键的内容，重要的是要清楚地了解信息安全问题的存在，并掌握信息安全所采用的技术，以保证信息的完整性和机密性。可以找到几种解决网络安全问题的方法：

2.1 网络安全解决方案

（1）边界防护系统建设：通过边界防护形成清晰、简洁的网络布局和系统架构，在网络边界部署安全防护设备（如防火墙、IPS、IDS、WAF网站应用级入侵防御设备等），将安

全风险和隐患降低到一个可以接受的水平，实现相关网络与系统之间严格访问控制的安全互连。

（2）进行安全域划分：全部设备均需分安全域部署，并在域间实施严格的访问控制策略，根据系统整体安全策略、内部数据流量和业务应用流程需求，对源/目的IP地址和端口进行限制，在网络层面实现系统整体的安全防护。

（3）防火墙技术的改进和健全：防火墙技术虽说无法完全的抑制恶意软件的攻击，但还是在一定范围内保护了计算机。所以，在设置防火墙时，设置有效的访问权限以防止未经授权的访问就非常重要。利用解锁计算机并引入隔离控制技术，恶意软件就可以难以进行恶意攻击，就可确保计算机系统内外的安全。

（4）量子加密技术的使用：加密技术使用量子作为密钥对信息进行编码，利用这项技术，连接的每一端都提供一个数字计算机信号，一个用户同意另一个用户接受。设备发送一系列量子数，计算机接收设备从两个字符串中提取对应的值并释放密钥，之后断开网络连接并创建一个新密钥。

（5）入侵检测技术：该技术用于检测电子计算机系统中是否存在违反安全策略的情况，这一技术能够及时检测并报告网络系统中的异常事件，从而减保护网络安全。

2.2 安全防护系统的正确选择

面对恶意攻击，可以针对不同的用户情况采用不同的安全措施，用户可依照自身实际情况选择安全系统，来确保自己的电脑不被黑客攻击。第一，根据用户自身级别判断，可以采取一些先进而简单的安全防范措施，例如：一个完整的数据安全系统可以保护整个企业的计算机网络以及保障所需的任何其他网络运行，免受外界环境因素的影响。在外界因素要进入内部之前，必须监控系统，如果审核失败，则将会将有问题的用户及其相关行为定义为疑似“第三方攻击”，并记录用户的 IP地址和行为，以防止此类攻击再次出现。其次，这对私人用户来说，不能使用大数据保护系统，从而多使用流行的安全系统，如杀毒360软件、云盾、都可以使用，但也必须遵循系统，在使用过程中定时更新，以确保保护效果，比如杀毒360软件就会提示用户定期的更新，这一目的就是为了扩充病毒库，让系统提供更多的防病毒保护，同时也防止一些特定的黑客进攻战术。.

2.3 核心数据的保护和加密

确保计算机安全系统的安全性以及可靠性。随着计算机网络技术的持续进步与发展，计算机安全变得越来越重要，各种加密技术也应运而生，其中密码加密就属于应用最广泛的一种加密技术，这一加密技术有很高的安全程度，密码加密就是数据加密。依照不同的网络加密要求，可对加密信息展开加密保护。因此，用户的某些部分也就可能对特定用户以外的用户不可用。因为有些用户不知道某些用户使用指南和特定用户操作，他们也就会被考虑到限制使用的人选中，被视作为指定用户之外的使用者，并且，一些用户会处理数据以防止泄露机密信息。另外，特定用户还可利用特殊的网络设备访问数据加密和设备翻译，确保选定的计算机用户可以在各种页面设置中安全地使用计算机数据。因此，只要在计算机网络上妥善解决这两个安全问题，就没有难处理的隐私问题，数字也就可以被加密。

2.4 提升专业素质，致力于创新

今天是互联网时代，信息在拼凑，数据在快速增长，各界都非常需要它，专业人员更应该具备通信系统和通信技术的综合理论，还需要通信领域的高水平技术人才具有研究设计、开发能力和创新能力。在提高通信系统工作团队的技术能力和业务素质的同时，专业人员还必须保持对通信技术传输技术和数据提取的分析和准备，改进传输技术研究，进一步提高运行效率。另外，在当前市场经济的影响下，通信系统更应进一步加大技术的创新，来符合数据增长的环境和人类对海量信息传播的需求。所以，在整体的通信系统中，需要格外的提高专家的发明技能，尽量地改进通信技术，进而提升通信系统的具体通信质量，以确保安全的通信数据和信息传输，保证传递的持续时间和准确性、质量。

2.5 通信网络管理系统改进

为确保电信管理的安全程度及有效性，完善通信网管体系，根据地方政府系统的结构特点，打造有针对性的通信网管体系，确保通信网管发挥作用。例如，如果信息中心的某个部门已经搭建了一个大数据处理平台，以确保一个大数据处理平台的信息技术咨询、决策发展战略、员工培训，确保对于每个部门的规划都有帮助，实现具体的区域战略规划。完善通信网络管理体系优化，促进通信网络系统的持续完善。随着，通信网络管理制度的有效运行，可及时发现通信网络系统的运行不足，便于技术人员及时进行技术升级与漏洞弥补。

3 结语

人类生活与网络的联系日益紧密，网络工具为人类生活带来便利的同时，也因安全问题给人类的信息安全带来威胁。通信工程网络安全技术的研究使用与人类生产生活紧密相连，实际生活中提高网络设计及使用技术，维护通信工程的网络安全，能够进一步确保网络的可靠性、保障人们生产生活顺力进行。

参考文献

[1]孙伟.论通信工程项目管理的安全管理措施[J].广东科技，2017，22（12）.

[2]姜山.网络通信安全及防火墙技术分析[J].网络安全技术与应用，2015，17（6）.

[3]高会生.电力系统通信的网络安全问题[J].都市家教电力信息化，2016，11（1）.

[4]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.

[5]梅岩.通信网络安全保障工程中的主动防御技术分析[J].中国新通信，2018，20（5）：4-5.

[6]吴天昊，岳一红.主动防御技术在通信网络安全保障工程中的应用研究[J].中国高新区，2018（18）：215，264.

[7]勉治宝.浅析通信工程网络安全问题与解决对策[J].建筑工程技术与设计，2015（25）：1025.