通信工程网络安全与对策探讨

王 菲
（西安明德理工学院，陕西 西安 710124）

摘要：随着信息技术的不断发展，人类社会正在经历着一场史无前例的深刻变革。当前，网络通信技术已经被广泛地运用在各个领域之中，比如说政治、经济、生产、军事等诸多领域之中，极大地改变传统事务处理方式，它的应用和发展在一定程度上推动了人类社会的进步和发展。与此同时，信息泄露问题也正在不断地发生，严重影响人们的正常生活。对此，本文就通信工程网络安全与对策进行简要分析，希望为广大读者提供一些有价值的借鉴和参考。

关键词：通信工程；网络安全；对策

随着个体安全意识的提高，信息安全问题越来越受到关注和重视，人们迫切需要可靠的、安全的网络通信。当前，信息安全问题已经上升到国家层面，必须准确了解和认识信息安全的表现方式和基本问题，掌握信息安全所依赖的信息网络化客观规律，从而使其作用充分发挥出来。本文首先就通信工程网络安全问题进行简要分析，之后针对这些问题，提出一些策略和方案，以此提升网络通信的安全性和可靠性。

一、通信工程网络安全问题分析

（一）盗取网络信息问题

当前，经过笔者实践调查发现，很多计算机用户在使用通信工程网络系统过程中，并不重视安全管理工作，管理模式简化，安装部署简单，这样做尽管能够缩短操作流程，但也埋下了一些隐患，很容易出现相关安全问题，并且不能对通信工程进行有效、全面的防护，很容易因为简陋的安全管理，导致信息泄露、黑客入侵等问题的发生。尤其是在使用第三方软件过程中，一旦这些软件自身存在一定的漏洞，本身的安全管理工作也存在问题，这就非常容易使一些木马病毒侵入到系统之中，从而对通信网络系统的正常运行造成影响，重要资料和数据丢失，对整个通信工程网络系统造成巨大的损害。

（二）通信工程网络自身存在一些问题

在通信工程中也会因为一些自身的问题而发生网络安全问题。在一般情况下，因特网采用的是 TPC/IP 协议，它的缺点和优点都非常明显，优点是具有较强的实用性，缺点是安全性较低，这就会导致其存在较多的安全隐患，容易发生网络安全问题。例如，在电子邮件方面，就非常容易遭受木马病毒或者黑客的不法侵入，导致重要邮件丢失，或者重要数据信息被盗取，从而产生严重网络安全问题，严重威胁用户的隐私安全。

（三）内部网络与外部网络之间存在一些问题

众所周知，互联网有内部网络和外部网络。为了防止发生信息被盗取等网络安全问题，一般情况下会对两者进行隔离。尽管这种方式能够在一定程度下保障用户的信息安全，防止方式网络安全问题，但也正因为此，内外网之间存在的隔离，导致在内外网连接过程中存在着一定的安全隐患，这对整个通信网络整体的运行造成严重的影响，降低了系统的安全性和可靠性。

（四）运用安全技术过程中存在一些问题

为了防止发生网络安全问题，造成信息泄露，会运用大量的安全技术，比如说防火墙、病毒检测、内存清理等技术，这些先进技术的运用能够对通信网络起到良好的保护作用，极大地提升安全性和可靠性，但在运用技术的过程中也存在一些问题，埋下一些隐患。一些用户为了防止信息被盗取，提升网络安全性，往往会使用大量的、先进的安全技术，但若不结合当前通信网络的实际情况，可能会引发更为严重的安全事故，造成通信网络无法正常运行，信息被盗取，为用户造成巨大的经济损失。

二、针对网络安全问题的具体有效对策

（一）强化通信安全管理制度

经过数据调查显示，截至 2023 年 6 月，中国共有域名 5800 万个，其中“CN”域名 2300 万个，占比 39.7%，“中国”域名 210 万个，其他顶级域名 3290 万个。根据《2023 年中国互联网网络发展状况统计报告》数据统计，截至 2023 年 6 月，中国网民规模已经突破 10 亿人，占全球网民总数量的 23%，位居世界第一位。随着我国网民数量的显著增加，我国信息盗取事件发生数量也在显著提升，对人们的生活造成了严重的影响。对此，应该更加重视和关注网络安全问题，并且针对其采取行之有效的方法，切实提升通信网络安全性和可靠性，确保通信网络整体的正常运行。

1. 运用安全交换机

随着计算机技术的不断发展，网络环境越来越严峻，网络病毒、黑客、软件漏洞等问题越来越多，企业和个人每年都会因此造成巨大的经济损失。针对这种情况，布置安全交换机就显得尤为重要。它是信息交换的核心设备，能够对相关数据进行存储和转发。在信息传输过程中，非常容易遭受到黑客的攻击，也会对交换机造成影响，甚至出现宕机的情况，因此，为了防止病毒、黑客的不法侵入，有必要使用安全的交换机，通过这样的方式，有效保障通信网络的安全和可靠

2. 加大安全管理力度

随着我国经济实力的不断提升，人们生活质量也随之提升，中国网民的数量位居世界第一，同时这也意味着网络安全问题更加严峻。因此，必须要重视和关注网络安全管理工作，应该采用行之有效的安全管理方式。不管是服务器应用服务，还是终端用户程序，这些都是运用在操作系统上的。对此，为了确保整个操作系统的安全，可以根据实际情况，建立访问控制制度；增加影响的安全补丁；建立对操作系统的监控系统等通过这样的方式，加大安全管理力度，避免信息泄露事件的发生。

3. 采用代理网关

当前，为了能够确保数据交换的安全性和可靠性，在网络安全管理工作领域之中，可以运用代理网关，这样做的好处在于网络数据包的变换不会再内外网之间进行，必须要通过代理网关，才能够访问因特网，从而极大地 提升永恒网络安全性和可靠性，有效防止数据信息被盗取。

4. 应用密钥管理方式

当前很多网络入侵者常常都是先对用户口令进行破译，破译成功之后，在入侵到网络系统之中，或者发现系统的薄弱部分、漏洞部分，以此为突破口进行入侵，从而对网络的安全造成极大的威胁。在此背景下，为了有效防止信息泄露，可以在系统和平台中设置密钥，开展和加强密码管理工作，在设置密钥口令过程中，

需要注意的是要尽可能提升口令的安全性和可靠性，尽可能增加口令位数，尽量不要选择一些常见密码，比如说生日、简单数字等，当作口令，也不要在不同系统中使用同样一个口令。尽量在无人状况下输入相关口令，并且要做到定期更换口令。此外，还可以利用口令破译程序对文件的安全性进行检测，通过多种方式和手段，确保信息安全，避免其被盗取。

（二）严格控制网络本身的安全性

为了提升网络自身的安全性，在实际工作中应该重视网络安全工作，严格开展安全管理工作，避免在通信工程网络信息传播过程中发生安全问题，从而在根本上提升网络信息的安全性和可靠性。

1. 使用数字签名技术

当前，为了确保文件信息在传输过程中的安全性和完整性，可以利用加密算法，通过特殊的符号或者代码形成电子密码签名，通过这样的方式，代替传统的书写签名或者相关印章，这种经过特殊方式制作而成的电子签名具有重要的作用，将其运用，可以提升数据传输过程中的安全性。此外还具有完善身份识别功能，并且不具有依赖性，在一定程度上能够加快交易的速度，确保交易的合理性和准确性。

2. 应用数字集群系统的安全技术

对数据集群系统来说，涉及信息安全的方面非常多，比如说加密方面、分级管理方面、日志管理方面等，可以将其系统划分为两种运营模式，分别是公网和专网，不管是哪种模式，都对通信覆盖率提出了很高的要求。因此，在一般情况下，数字集群系统主要是运用在应急通信领域，业务量往往会具有突发性特征，因此，为了更为有效的提升其安全性，有必要做好控制拥塞工作，根据系统的运行特点、安全问题发生规律等，采用有效的手段和方式，去防止安全事故，从而提升系统运行的安全性和可靠性。

（三）采用先进的隔离技术

为了提高通信网络工程中网络安全性，可以整合不同的系统，运用隔离技术，以此提升整个通信网络的安全性，借助外端的客户端，顺利实现网布网线与内部之间的交换处理，有效解决当前的网络安全问题。在隔离技术的助力下，确保内外网之间安全、可靠。首先，对于用户的计算机来讲，首先需要的就是要做好认真工作，若与之前登录的服务器不同，应该禁止接入该网络和开放网络端口，若用户已经进入，应该及时的提出预警信息。其次，针对数据库操作期间的记录，要做好排序工作，按照顺序进行处理，并定期进行服务器数据信息的内外网互换，将相关序列发送到另外一个服务器上，并且做好标记。若用户的违规不当或者存在违规操作的情况，就要停止与外网之间的连接。最后，要详细记录用户登录服务器的登录时间，并且对其进行全程监控，在客户端使用安全系统，从而确保服务器能够正常联网，并且合规合法使用。在这里还需要注意的是，若安全系统关闭，无法接受序列信息，应该立即开展安全系统处理工作。

（四）做好备份工作

经过数据调查发现，对内网造成的安全威胁的因素网络存在系统内部。黑客在对局域网进行攻击的过程中，一般情况下会选择控制系统中的一台计算机，并以此为基础对内部其他计算机进行入侵。因此，为了有效防止黑客的入侵，应该加强内网的安全措施。由于一些重要的信息通过内网进行保存和传输，一旦遭到黑客的入侵，将会对个人以及集体造成巨大的影响，因此，为了防止重要信息、数据等遭受到损失，可以采取实时备份的方式，降低损失程度，尽管系统遭受到严重的损害，但一些重要数据不会丢失。此外，应该对局域网内部进行严格审查，针对一些闲置的网络服务器，应该及时予以关闭，通过这样的方式确保网络的安全和可靠。

（五）运用隔离技术

网络工作人员也可以运用隔离技术，以此将内外网进行隔离开，从而增强内网的安全性。在运用这项技术之后，若网络系统在规定时间内不能收到发来的信息，则会被判定为恶意攻击，从而关闭系统。

（六）提升设计人员专业素养，选择合理配置

在设计计算机系统过程中，设计人员自身的必须要具备高超的专业素养和技术水平，他们需要进行全面的考虑，确保系统整体上的科学合理。因此，为了确保通信工程网络安全，有必要提升设计人员专业素养。同时也要选择合理的计算机配置，这是提升网络安全的重要基础。

（七）及时革新防火墙技术

确切来讲，防火墙技术是一个系统，它位于被保护网络与其他网络之间，它的主要功能就是对访问进行控制，防止非法入侵和非法的信息传递，它并不是简单的一种软件或者硬件，而是软件和硬件再加上一组安全策略的集合。将其运用到通信工程网络之中，能够有效阻止非法侵入，对整个系统起到良好的保护作用。但是，当前的防火墙技术存在一定的欠缺，无法有效达到理想效果。因此，在设置防火墙过程中，要重点注意访问权范围，通过这样的方式提升抵御力度，确保信息在传递过程中的安全。

（八）强化检测技术

计算机的发展为人们的生活带来了巨大的便利，同时计算机病毒也在不断地发展，随着编程手段的不断创新，因特网的广泛使用，计算机病毒空前活跃，对计算机安全网络造成了巨大的威胁。而计算机检测技术的运用能够主动对入侵者的入侵痕迹进行探测，能够起到良好的主动防御作用。因此，有必要运用计算机检测技术，并且不断进行革新和强化，确保恶意软件、病毒在入侵系统时能够及时通知，并且对相关漏洞进行不断巩固和修复，从而提升网络安全性。

三、结束语

当前，随着信息技术的不断发展，给人类社会带来了巨大的发展机遇，同时也带来了严峻的安全挑战。通信工程网络面临各种各样的安全威胁，比如说计算机病毒、黑客不法侵入、信息泄露等问题，因此，有必要加强安全管理工作，选择和采取科学、先进的安全管理技术，从根本上提升网络的安全性和可靠性，为人们生活发展奠定坚实的基础。

参考文献：

[1] 徐璐 . 民航网络通信工程建设的研究 [J]. 网络安全技术与应用，2023（04）：130-131.

[2] 胡克汉 . 通信工程网络安全与对策分析 [J]. 网络安全技术与应用，2022（11）：169-171.

[3] 王磊 . 通信工程技术在多网融合环境下的应用分析 [J]. 长江信息通信，2022，35（02）：216-217+223.

[4] 杨瑀 . 人工智能技术赋能通信工程产业的逻辑与路径 [J]. 营销界，2021（31）：103-104.

[5] 刘汉君 . 通信线路施工与安全管理 [J]. 科技风，2021（12）：114-115.

[6] 黄晓龙 . 通信工程网络安全与对策探讨 [J]. 电子测试，2021（07）：129-130+128.

[7] 屈俊玲 . 多网融合在通信工程中的应用分析 [J]. 数字通信世界，2020（09）：191-192+104.