通信工程网络安全与对策探讨

李伟辉
（广东南方电信规划咨询设计院有限公司，广东　深圳　518000）

【摘　要】随着信息技术的迅猛发展，通信工程在现代社会中扮演着至关重要的角色。然而，网络安全问题也随之而来。本文对通信工程网络安全问题进行了深入分析，并提出了相应的对策。通过积极采用安全交换机系统、严格操作系统的安全管理、应用代理网关和重点应用密钥管理方式等预防措施，以及积极使用数字签名技术、数字集群系统的安全技术和合理使用量子密码加密技术等控制措施，可以有效解决通信工程网络安全问题。同时，本文还强调了先进的隔离技术措施和基本性的安全技术的积极应用，以提升通信工程网络的整体安全性。

【关键词】通信工程；网络安全；信息盗取；隐患；内外网；安全技术

引言：

无论是企业的数据传输、个人的通信交流还是政府的信息管理，通信工程网络承载着大量敏感和重要的数据。然而，随之而来的网络安全问题也日益突出。网络信息盗取、系统漏洞、内外网安全等问题威胁着通信工程的安全性和稳定性。为了确保通信工程网络的安全，必须积极探索和采取相应的对策。本文将深入分析通信工程网络安全问题，并提出一系列针对性的对策，以应对不断演变的威胁和挑战。

一、通信工程的基本概念

通信工程是一门涉及设计、建设和维护通信系统的工程学科，旨在通过利用通信技术和设备，实现信息的传输和交流。通信工程的作用是建立可靠的通信网络，促进人们之间的沟通和信息的传递。随着信息技术的快速发展，通信工程在现代社会中扮演着重要的角色。通信工程的发展历程可以追溯到电信行业的兴起。从最初的有线电报和电话系统到现代的移动通信、卫星通信和互联网，通信工程在不断演进和创新。它涵盖了多种技术领域，包括电信、计算机网络、无线通信和光纤通信等。通信工程在现代社会中的重要性不可忽视。它为人们提供了便捷和高效的通信手段，改变了人们的生活方式和工作方式。它支撑着各行各业的信息交流和业务运营，涵盖了政府机构、企业、学校、医疗机构以及个人生活等方方面面。随着通信技术的不断创新和普及，通信工程面临着一系列的挑战和安全问题。网络安全成为通信工程中的重要议题之一。了解通信工程的基本概念和背景知识，有助于我们更好地理解和应对通信工程中的网络安全问题。

二、通信工程网络安全问题分析

（一）网络信息盗取问题

网络信息盗取是通信工程网络安全中的重要问题，它涉及黑客攻击、恶意软件和社会工程等方式对通信工程网络中的信息进行非法获取的情况。这种信息盗取行为可能对个人、组织和国家造成严重的损失和风险。黑客攻击是一种常见的信息盗取手段，黑客通过网络渗透和攻击技术，窃取目标网络中的敏感信息，例如个人身份信息、财务数据和商业机密等。恶意软件（如病毒、木马和间谍软件）则以隐藏在正常应用程序中的形式，通过感染计算机系统来获取用户的敏感信息。此外，社会工程是指通过欺骗、假冒或诱导等手段获取用户信息，如钓鱼邮件、假冒网站和电话诈骗等。导致信息盗取的原因主要包括安全漏洞的存在、弱密码的使用、不安全的网络传输和缺乏安全意识等。信息盗取可能导致个人隐私泄露、财务损失、商业机密泄露以及国家安全威胁等严重后果。

（二）网络本身存在潜在隐患

通信工程网络本身存在潜在隐患是网络安全中的一大挑战，这些隐患包括系统漏洞、弱口令和未授权访问等问题。这些隐患可能导致恶意用户或攻击者入侵网络系统、获取敏感信息或破坏网络的正常运行。首先，软件或操作系统中的漏洞可能被黑客利用，从而使得网络系统容易受到攻击。为了应对这个问题，通信工程需要定期进行系统漏洞扫描和安全评估，并及时安装软件补丁来修复已知漏洞。其次，弱

口令也是网络安全的薄弱环节。使用弱口令或默认密码的用户容易受到密码破解或暴力破解的攻击。为了增强口令的安全性，通信工程应要求用户使用复杂且难以猜测的密码，同时设置密码策略，包括密码长度、复杂度和过期时间等。此外，未授权用户或非法用户可能通过绕过安全控制手段访问网络资源或系统。为了防止未授权访问，通信工程应采用访问控制机制，如身份认证和授权管理，限制用户只能访问其授权范围内的资源。

（三）内外网的安全问题

随着信息技术的迅速发展和网络的广泛应用，内外网的互联和数据传输成为不可避免的需求。然而，内外网之间的互联也带来了一系列的安全挑战和威胁，需要采取相应的安全措施来保护网络和数据的安全。首先，内外网的互联可能会导致未授权访问的风险。未经授权的用户或设备可能会试图进入内部网络，获取敏感数据或进行恶意活动。因此，建立适当的访问控制机制是非常重要的。可以使用防火墙、入侵检测系统和访问控制列表等技术来限制内外网之间的访问，并确保只有经过授权的用户或设备才能进行通信和数据传输。其次，内外网之间的数据传输需要保证机密性和完整性。敏感数据的传输可能受到窃听、篡改或伪造的威胁。为了防止这些风险，可以采用加密技术来保护数据的机密性，并使用数字签名或消息认证码等技术来验证数据的完整性。此外，建立安全的虚拟专用网络（VPN）连接可以提供加密的通信通道，确保内外网之间的数据传输安全可靠。另外，内外网的安全问题还涉及恶意软件和网络攻击的风险。恶意软件可能通过内外网的互联传播，对网络系统和数据造成损害。因此，应该采取有效的防病毒软件、入侵检测和防御系统来及时发现和应对潜在的威胁。同时，进行定期的安全漏洞扫描和更新是必要的，以确保网络设备和系统的安全性。

（四）安全技术应用的问题

通信工程中，安全技术的应用是确保网络和数据安全的重要方面。然而，安全技术的应用也面临一些问题和挑战，需要针对性地进行优化和改进。首先，安全加密算法的应用是保护数据机密性的关键手段。然而，随着计算能力的提升和攻击技术的演变，传统的加密算法可能面临被破解的风险。因此，选择强度更高的加密算法，如 AES（高级加密标准）和 RSA（一种非对称加密算法），以及采用合适的密钥管理和更新策略，是提高加密算法应用效果的重要措施。其次，身份认证和访问控制是防止未经授权访问的关键技术。然而，传统的用户名和密码认证方式存在被猜测、共享或泄露的风险。为了提高身份认证的安全性，可以引入多因素身份认证，如使用指纹、虹膜或声纹等生物特征进行验证。同时，采用智能卡、USB 令牌或硬件安全模块等物理设备作为身份认证的辅助手段，可以有效提升认证的可靠性。

另外，访问控制的应用也面临一些问题。例如，权限过度授予和缺乏细粒度访问控制可能导致数据泄露和未经授权的操作。因此，需要建立合理的访问控制策略，包括基于角色的访问控制（RBAC）和基于策略的访问控制（PBAC）等，以确保用户只能获得所需的最低权限，并且对敏感数据进行细致的控制和监管。此外，安全技术的应用还需要考虑系统的兼容性和可扩展性。不同厂商和系统之间的兼容性问题可能会影响安全技术的有效应用。因此，需要推动标准化工作，促进不同安全技术之间的互操作性。同时，为了适应通信工程中不断增长的网络规模和复杂性，安全技术也需要具备良好的可扩展性，能够应对未来的安全挑战。

三、通信工程中网络安全问题的对策

（一）预防出现信息盗取的问题

1. 积极使用安全交换机系统：安全交换机系统是一种可以提供网络流量监测、访问控制和安全审计等功能的设备。通过在网络中引入安全交换机系统，可以实时监测网络流量，检测并阻止潜在的恶意行为，从而减少信息盗取的风险。2. 严格进行操作系统的安全管理：操作系统是通信工程网络的核心组成部分，保障操作系统的安全至关重要。应该及时安装操作系统的安全补丁和更新，禁用不必要的服务和功能，设置强密码，并定期对系统进行漏洞扫描和安全评估，确保操作系统的安全性。3. 采用代理网关：代理网关是位于内部网络与外部网络之间的中间设备，可以过滤和监控网络流量，阻止恶意访问和数据泄露。通过配置代理网关，可以限制对内部网络的访问，并对外部网络的访问进行审计和控制，有效防止信息被盗取。4. 重点应用密钥管理方式：密钥管理是通信工程中保障数据安全的重要环节。采用合理的密钥管理方式，如对称密钥和非对称密钥的使用，可以加强数据的加密和解密过程，保障通信过程中数据的机密性和完整性。

（二）严格控制网络本身的安全性

为了确保通信工程网络的安全性，除了预防信息盗取的问题外，还需要严格控制网络本身的安全性。

以下是一些具体的对策和措施：1. 积极使用数字签名技术：数字签名技术可以用于验证数据的真实性和完整性，防止数据被篡改。在通信工程中，可以使用数字签名技术对重要数据、软件和通信消息进行签名和验证，确保数据在传输和存储过程中不被篡改或伪造。2. 应用数字集群系统的安全技术：数字集群系统是一种将多个计算节点组成的集群，通过分布式计算和冗余备份来提高系统的可用性和安全性。在通信工程中，可以利用数字集群系统的安全技术，如节点身份认证、数据加密和分布式访问控制等，提高网络的抗攻击能力和数据的保密性。3. 合理使用量子密码加密技术：量子密码加密技术是一种基于量子力学原理的加密方法，具有很高的安全性和抗量子计算攻击能力。通信工程可以合理应用量子密码加密技术，对敏感数据和通信进行保护，防止被窃听和破解。通过积极采用上述措施，可以加强通信工程网络本身的安全性。然而，随着网络攻击技术的不断演进，单一的安全措施可能不足以应对复杂的安全威胁。因此，综合采用多种安全技术和方法，建立完善的安全体系，是保障通信工程网络安全的关键。同时，还应定期进行安全评估和漏洞扫描，及时修补和更新系统，以应对新型攻击和漏洞的出现。只有不断提升网络本身的安全性，才能确保通信工程的可靠运行和信息的安全传输。

（三）积极采用先进的隔离技术措施

为了进一步提升通信工程网络的安全性，采用先进的隔离技术是一种有效的策略。以下是一些具体的隔离技术措施：1. 网络隔离：网络隔离是通过将网络划分为多个独立的区域或子网，限制不同区域之间的通信和访问，从而控制网络流量的传播范围。可以使用虚拟局域网（VLAN）技术、网络地址转换（NAT）和访问控制列表（ACL）等方法实现网络隔离。通过网络隔离，即使发生一部分网络区域的安全漏洞，也能够限制攻击者的行动范围，保护其他区域的安全。2. 安全隔离区域：安全隔离区域是将关键系统和数据集中在受控的物理或逻辑环境中，与其他非关键系统和数据进行隔离。可以使用安全隔离区域来划分不同的安全等级和访问权限，确保只有经过授权的人员才能访问和操作关键系统和数据。常见的安全隔离区域包括安全操作中心（SOC）、机密数据中心和授权访问区域等。3. 物理隔离：物理隔离是通过物理手段来隔离关键设备和系统，防止未经授权的物理访问。例如，将服务器和网络设备放置在安全的机房中，采用门禁、摄像监控和防火墙等物理安全措施，确保只有授权人员才能进入机房，并保护设备免受物理攻击。

（四）积极采用基本性的安全技术

在通信工程中，积极采用基本性的安全技术是确保网络安全的关键一环。以下是一些基本性的安全技术及其应用和部署策略：1. 防火墙：防火墙是网络安全的第一道防线，用于监控和控制网络流量，阻止未经授权的访问和恶意活动。在通信工程中，应合理部署防火墙，根据网络拓扑和安全需求设置访问规则，对网络通信进行过滤和检查，防止恶意攻击和未经授权的访问。2. 入侵检测系统（IDS）：入侵检测系统可以监测和分析网络中的异常行为和攻击活动，并及时发出警报。通信工程中，应积极部署入侵检测系统，包括网络入侵检测系统（NIDS）和主机入侵检测系统（HIDS），以实时监测和识别潜在的入侵事件，并采取相应的响应措施。3. 反病毒软件：恶意软件和病毒是网络安全的常见威胁，能够导致数据损坏、系统崩溃和信息泄露等问题。通信工程中，应积极采用可靠的反病毒软件，及时更新病毒库和进行病毒扫描，以发现和清除潜在的恶意软件和病毒，保护系统和数据的安全。除了上述基本性的安全技术外，通信工程还应考虑其他安全技术的应用，如身份认证、访问控制、加密通信和安全日志管理等。综合采用这些安全技术，可以提供多重防御和保护机制，增强通信工程的安全性和抵御能力。

结束语：

总之，通信工程在现代社会中具有重要意义，但也面临着各种安全挑战。为确保通信网络的安全性，必须采取综合性的措施，包括技术手段、管理策略和人员培训等方面的改进。通过不断加强网络安全意识、应用先进的安全技术和加强管理，我们可以建立更可靠、安全的通信工程网络，为社会发展和信息交流提供有力支持。

参考文献：

[1] 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.

[2] 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.

[3] 刘浩朋 . 通信工程网络安全与对策探讨 [J]. 信息通信，2014(04)：222-223.

[4] 杨振宇，许晓川 . 通信工程网络安全与对策探讨 [J]. 中国科技投资，2013(14)：140.