工程管理
Journal of Project Management
第 6 卷◆第 2 期◆版本 1.0◆2025 年
文章类型：论文|刊号（ISSN）：2737-4580(P) / 2737-4599(O)

计算机网络工程与信息安全策略分析

吴小胜
达州市中西医结合医院
DOI:10.12238/jpm.v6i2.7745
[摘　要] 计算机网络工程发展迅速，信息安全成为关键。阐述网络工程现状，包括其架构与技术应用。分析信息安全面临的威胁，如网络攻击、数据泄露等。探讨应对策略，涵盖技术手段、管理措施等，强调信息安全对网络工程稳定运行的重要性。
[关键词] 计算机网络工程；信息安全；威胁；策略；技术手段

Analysis of Computer Network Engineering and Information Security Strategy

Wu Xiaosheng
Dazhou City Hospital of Integrated Traditional Chinese and Western Medicine
[Abstract] With the rapid development of computer network engineering, information security has become the key.Explain the current situation of network engineering, including its architecture and technology application.Analyze the threats facing information security, such as network attacks, data leakage, etc.Discuss coping strategies, covering technical means and management measures, and emphasize the importance of information security to the stable operation of network engineering.
[Key words] computer network engineering; information security; threat; strategy; technical means

引言：

在当今数字化时代，计算机网络工程无处不在，从企业运营到个人生活。然而，随着网络的普及，信息安全问题日益凸显。网络工程面临着各种威胁，这不仅影响着用户的隐私和数据安全，也可能对企业和社会造成巨大损失。因此，深入分析计算机网络工程中的信息安全策略具有重要意义。

1.计算机网络工程概述

1.1 网络工程架构

网络工程架构是计算机网络工程的基石。它涵盖了从网络的物理布局到逻辑结构的各个方面。在物理层面，涉及到网络设备的选型与布局，如路由器、交换机等设备的放置位置，要考虑到信号传输的稳定性、覆盖范围等因素。例如在大型企业网络中，核心交换机往往位于数据中心，以保障数据的高速交换与集中管理。在逻辑结构方面，网络分层架构如 OSI 七层模型或 TCP/IP 四层模型，明确了不同层次的功能与交互方式。每一层都有其特定的任务，从物理层的信号传输，到应用层的用户交互。合理的网络工程架构能够提高网络的可扩展性、可维护性以及性能。它能够适应不同规模和需求的网络环境，无论是小型办公网络还是大型的云计算数据中心网络，都是构建高效、稳定网络的关键要素。

1.2 网络工程主要技术

网络工程主要技术是推动计算机网络工程不断发展的核心动力。其中，网络传输技术是基础，包括有线传输技术如光纤、双绞线等，以及无线传输技术如 Wi - Fi、蓝牙等。光纤以其高速、低损耗的特性，广泛应用于长距离、大容量的数据传输，如电信运营商的骨干网络。而 Wi - Fi 则方便了移动设备的接入，满足了人们随时随地联网的需求。网络协议技术也是关键，像 TCP/IP 协议，它是互联网通信的标准协议，确保了不同设备、不同网络之间的互联互通。路由技术则决定了数据在网络中的传输路径，动态路由协议能够根据网络的实时状态自动调整路由，提高网络的可靠性和效率。交换技术则实现了数据在局域网内的快速转发，减少冲突，提高网络的带宽利用率。这些技术相互配合，共同构建起功能强大的计算机网络工程。

2.信息安全面临的威胁

2.1 网络攻击类型

网络攻击类型多种多样，且日益复杂和隐蔽。其中，拒绝服务攻击（DoS）是一种常见的攻击方式，攻击者通过发送大

量的请求，使目标服务器资源耗尽，无法正常提供服务。例如，分布式拒绝服务攻击（DDoS）利用大量被控制的僵尸主机同时向目标发动攻击，其攻击流量巨大，能够轻易使小型企业的网站瘫痪。恶意软件攻击也是极为严重的威胁，如病毒、木马等。病毒能够自我复制并传播，感染计算机系统，破坏文件、窃取数据等。木马则通常伪装成正常的程序，一旦用户运行，就会在后台悄悄运行，为攻击者打开控制计算机的后门。还有网络钓鱼攻击，攻击者通过伪造合法的网站或邮件，诱导用户输入敏感信息，如账号密码等，从而窃取用户的隐私数据。这些网络攻击类型不断演变，对信息安全构成了巨大的挑战。

2.2 数据泄露风险

数据泄露风险是信息安全领域不容忽视的问题。在当今数字化时代，数据的价值极高，无论是企业的商业机密、用户的个人信息还是国家的机密数据等。数据泄露可能发生在多个环节。首先，在数据存储环节，如果存储系统的安全防护不足，如数据库没有进行严格的访问控制，黑客就可能通过漏洞入侵并窃取数据。其次，在数据传输过程中，若采用的加密技术不完善或者被破解，数据就可能被拦截并泄露。例如，一些企业在传输敏感数据时没有使用足够强度的加密算法，导致数据在传输过程中被窃取。再者，内部人员的不当操作也可能导致数据泄露，如员工误将包含敏感信息的文件发送给错误的对象，或者内部人员出于私利故意泄露数据等，这些情况都增加了数据泄露的风险。

2.3 内部安全隐患

内部安全隐患是信息安全中容易被忽视但却危害巨大的部分。内部人员由于其对企业内部网络和系统的熟悉程度，一旦出现安全问题，往往会造成严重的后果。一方面，员工的安全意识不足是一个重要隐患。例如，员工可能会随意点击可疑的邮件链接或下载不明来源的软件，这可能会导致恶意软件入侵企业内部网络。另一方面，内部人员的权限管理不当也存在风险。如果权限分配不合理，一些员工可能拥有过高的权限，能够访问和修改一些本不应该接触的数据，这就增加了数据被误操作或恶意篡改的可能性。此外，内部网络的安全配置不当也是内部安全隐患之一，如内部网络没有进行有效的隔离，一旦某个终端被感染，就可能迅速在内部网络中传播，影响整个企业的信息安全。

3.信息安全策略的技术手段

3.1 加密技术

加密技术是保障信息安全的重要技术手段。它通过将原始数据转换为密文的形式，使得只有拥有正确密钥的接收者才能将其还原为原始数据。在现代信息安全体系中，加密技术应用广泛。对称加密算法如 AES（高级加密标准），其加密和解密使用相同的密钥，具有加密速度快的特点，适用于大量数据的加密。例如在本地存储数据时，可以使用 AES 算法对数据进行加密，防止数据被窃取后能够被轻易解读。非对称加密算法如 RSA，它使用公钥和私钥对，公钥用于加密，私钥用于解密。这种算法在网络通信中的安全认证方面应用广泛，如在 SSL/TLS 协议中，通过非对称加密来实现服务器和客户端之间的身份认证和密钥交换。哈希函数也是加密技术的一部分，它可以将任意长度的数据转换为固定长度的哈希值，用于验证数据的完整性。加密技术的不断发展和创新，为信息安全提供了坚实的技术保障。

3.2 防火墙设置

防火墙设置在信息安全防护中起着至关重要的作用。防火墙是一种位于内部网络和外部网络之间的网络安全系统，它可以根据预设的规则来控制网络流量的进出。在设置防火墙时，首先要明确防护的目标。对于企业网络来说，要保护内部的服务器、数据库等重要资源免受外部网络的非法访问。例如，通过设置访问控制列表（ACL），可以允许或禁止特定 IP 地址或网络段的访问。其次，要根据网络的实际需求配置防火墙规则。例如，对于 Web 服务器，只允许外部网络对其 80 端口（HTTP）和 443 端口（HTTPS）的访问，其他端口则禁止访问。同时，防火墙还可以进行深度包检测，对数据包的内容进行分析，防止恶意软件通过伪装的正常流量进入内部网络。此外，防火墙的日志功能也很重要，它可以记录网络访问的相关信息，以便在发生安全事件时进行审计和追踪。

3.3 入侵检测系统

入侵检测系统（IDS）是信息安全策略中不可或缺的技术手段。IDS 能够对网络或系统中的可疑活动进行检测并发出警报。它主要分为基于主机的入侵检测系统（HIDS）和基于网络的入侵检测系统（NIDS）。HIDS 主要关注单个主机的活动，它通过监测主机上的系统文件、进程、网络连接等信息，来判断是否存在入侵行为。例如，当有恶意程序试图修改系统关键文件时，HIDS 能够检测到并及时发出警报。NIDS 则是对网络流量进行监测，它可以分析网络数据包的特征，识别出异常的流量模式。例如，当网络中出现大量来自同一源地址的异常连接请求时，NIDS 会判断为可能的入侵行为并报警。入侵检测系统还可以与防火墙等其他安全设备协同工作，当检测到入侵行为时，可以通知防火墙采取相应的措施，如阻断可疑的网络连接，从而提高整个网络的安全性。

4.信息安全的管理措施

4.1 安全制度建立

安全制度建立是信息安全管理的基础。一套完善的安全制度应该涵盖多个方面。首先，要明确信息安全的目标和策略，

规定企业或组织在信息安全方面的总体方针，例如确定数据保护的级别、安全事件的响应流程等。其次，要对人员的行为进行规范，包括员工的网络使用规范、数据访问规范等。例如，禁止员工在工作电脑上安装未经授权的软件，限制员工对敏感数据的访问权限等。再者，安全制度还应包括设备管理规范，如规定网络设备、服务器等的维护周期、更新策略等。此外，安全制度还需要明确安全责任的划分，确保在发生安全事件时能够迅速确定责任主体。同时，安全制度要定期进行审查和更新，以适应不断变化的信息安全环境。

4.2 人员安全意识培养

人员安全意识培养是信息安全管理的关键环节。由于人是信息安全中最薄弱的环节，提高人员的安全意识能够有效降低安全风险。首先，要进行安全知识的培训，包括网络安全基础知识、常见的网络攻击类型、如何识别和防范等。例如，通过培训让员工了解网络钓鱼的手段，从而避免点击可疑的邮件链接。其次，要进行安全意识的宣传，通过内部通告、宣传海报等多种形式，营造浓厚的安全文化氛围。例如，在企业内部张贴关于信息安全的标语，提醒员工注意保护数据安全。再者，要定期进行安全演练，模拟安全事件的发生，检验员工的应对能力。例如，进行模拟的网络攻击演练，让员工熟悉安全事件的处理流程，提高他们的应急反应能力。

4.3 安全审计与监控

安全审计与监控是信息安全管理的重要保障措施。安全审计是对网络和系统中的活动进行记录和分析，以便发现潜在的安全问题。在安全审计过程中，要确定审计的范围，包括网络设备、服务器、应用程序等。例如，对企业的数据库服务器进行审计，记录所有的数据库操作，如查询、插入、删除等操作的时间、用户等信息。监控则是实时地对网络和系统的运行状态进行监测，发现异常情况及时处理。例如，通过网络监控工具监测网络的流量、带宽利用率等指标，一旦发现异常的流量高峰，就要进一步分析是否存在网络攻击。安全审计与监控还可以为安全事件的调查提供依据，当发生安全事件时，可以通过审计和监控记录来追溯事件的发生过程，确定责任人和原因。

5.信息安全策略对网络工程的意义

5.1 保障网络稳定运行

信息安全策略对网络工程的稳定运行有着不可替代的意义。在网络工程中，网络的稳定性是至关重要的。信息安全策略通过防范各种网络攻击，如病毒入侵、恶意软件攻击等，避免这些攻击对网络设备和系统造成破坏，从而保障网络的正常运行。例如，防火墙的设置可以阻止外部的恶意流量进入网络，防止网络设备因遭受攻击而出现故障。加密技术的应用可以确保数据在传输和存储过程中的安全性，防止数据被篡改或破坏，这有助于维持网络的正常通信和数据交互。同时，入侵检测系统能够及时发现潜在的安全威胁并采取措施，避免安全问题进一步恶化影响网络的稳定运行。

5.2 提升用户信任度

信息安全策略能够显著提升用户对网络工程的信任度。在当今数字化时代，用户对于网络安全的关注度极高。如果一个网络工程能够有效地实施信息安全策略，如采用先进的加密技术保护用户数据、建立完善的安全制度防止数据泄露等，用户就会更加放心地使用该网络服务。例如，在电子商务领域，用户在进行在线交易时，如果网站能够展示其采用了严格的信息安全措施，如安全套接层（SSL）证书等，用户就会更愿意提供自己的个人信息和进行交易。对于企业网络来说，保障员工和合作伙伴的数据安全也能够提升他们对企业网络的信任度，促进企业内部的协作和外部的合作关系。

5.3 促进网络工程发展

信息安全策略对网络工程的发展有着积极的促进作用。随着网络技术的不断发展，网络工程面临着越来越多的挑战，而信息安全问题是其中的关键。有效的信息安全策略能够吸引更多的用户和投资者，因为他们看到了网络工程在安全方面的保障。例如，一些新兴的云计算服务提供商，如果能够提供可靠的信息安全策略，就能够吸引更多的企业将业务迁移到云端。同时，信息安全策略的发展也推动了网络工程技术的创新，如加密技术、入侵检测技术等的不断发展，促使网络工程不断适应新的安全需求，从而在技术和应用方面不断发展和进步。

结束语：

计算机网络工程中的信息安全是一个复杂而又至关重要的问题。通过对信息安全面临威胁的分析，以及从技术手段和管理措施等方面制定策略，可以有效保障网络工程的安全稳定运行。这不仅有助于保护用户的隐私和数据安全，还能推动整个计算机网络工程不断发展，适应日益增长的数字化需求。

[参考文献]

[1]郝景昌，徐李阳，赵文华，等.大数据时代计算机网络信息安全与防护[J].数字技术与应用，2023（4）：219-221.

[2]王娜，王新，杨飞，等.全方位网络信息安全防护体系研究[J].邮电设计技术，2023（8）：29-32.

[3]杨忠铭.计算机网络信息安全及其防火墙技术应用[J].数字通信世界，2023（1）：126-128.

[4]王文江，柏赫，刘鑫，等.计算机网络安全入侵检测技术研究[J].中国新通信，2023（4）：102-104.