电子信息工程中的网络安全防护技术研究

马　亮
邯郸市房产信息中心　河北　邯郸　056000

摘　要：电子信息工程中的网络安全防护技术，是保障信息安全可用、事关社会稳定发展的重要技术。本文深入探讨了防火墙技术、入侵检测与防御系统、加密技术、虚拟专用网络（VPN）技术及身份认证与访问控制等核心防护手段。通过理论分析与案例研究，分析了防护技术在防御网络攻击、保护数据安全、维护系统完整性方面的重要作用。随着技术的不断进步，网络安全防护技术需要不断改进、持续创新、领先一步，以应对日益复杂多变的网络威胁。

关键词：网络安全；信息工程；防护技术；发展趋势

1 网络安全防护技术基础理论

网络安全防护技术基础理论主要关注信息的保密性、完整性和可用性。从技术层面看，网络安全防护涉及多个方面。首先，防火墙技术是在两个网络之间强制实施访问控制策略的关键系统，分为包过滤防火墙和应用代理防火墙两大类。其次，加密技术能够保护数据的传输安全，防止数据在传输过程中被窃取或篡改。另外，入侵检测技术能够及时发现并响应网络入侵行为，从而保障网络系统的安全。操作系统安全配置也是不可忽视的一环，通过合理配置操作系统，能够有效减少安全漏洞。最后，端口扫描、漏洞扫描等技术能够发现系统中的潜在弱点，并采取相应的措施进行加固。

2 电子信息工程中的网络安全威胁分析

2.1 网络安全威胁的类型

在电子信息工程中，网络安全威胁的类型多种多样。常见的包括病毒和恶意软件，它们能够侵入计算机系统，破坏数据、监视用户活动或控制受感染的计算机。网络钓鱼通过伪装成合法机构或个人，获取敏感信息，如用户名、密码等。DDoS攻击则通过超负荷请求使目标服务器或网络不可用[1]。数据泄露、无线网络攻击、弱密码和身份验证漏洞、云安全威胁以及内部威胁等，也是电子信息工程中常见的网络安全威胁类型。

2.2 网络安全威胁的来源

网络安全威胁的来源广泛，包括恶意软件（如病毒、蠕虫、木马等）、网络钓鱼攻击者、中间人攻击者、分布式拒绝服务攻击者等。软件和硬件缺陷、环境因素（如电磁波辐射、自然灾害等）以及人为因素（如操作失误、违法犯罪行为等）也可能成为网络安全威胁的来源。内部威胁同样不容忽视，合法用户可能利用权限进行恶意活动或错误操作，对系统安全构成威胁。

2.3 网络安全威胁的影响

网络安全威胁对电子信息工程的影响深远。一方面，数据泄露和恶意软件可能导致敏感信息被未经授权的人员获取，对个人隐私和企业安全造成严重影响。另一方面，网络钓鱼和中间人攻击可能破坏系统的完整性，导致服务中断或数据篡改。DDoS攻击利用可能导致系统资源耗尽或系统崩溃，影响业务的正常运行。内部威胁则可能导致用户遭受重大经济损失或声誉损害。

3 电子信息工程中的网络安全防护技术

在当今数字化的时代，电子信息工程已成为推动社会发展和进步的重要力量。从智能手机、智能家居到工业自动化、医疗设备，电子信息工程的应用无处不在。然而，随着网络的普及和信息技术的飞速发展，网络安全问题也日益凸显，给电子信息工程带来了严峻的挑战。网络安全不仅关系到个人隐私和财产安全，还关乎国家的经济发展和社会稳定。因此深入研究电子信息工程中的网络安全与防护技术具有重要的现实意义。

3.1 防火墙技术

防火墙技术是一种位于计算机和它所连接的网络之间的软件或硬件设备，用于阻止未经授权的网络访问。防火墙技术是建立在网络技术和信息安全技术基础上的应用性安全技术。防火墙并非单纯的软件或硬件，而是软件和硬件加上一组安全策略的集合。防火墙的作用可以类比于古时候人们砌在寓所之间的砖墙，用于防止火灾的蔓延。在网络环境中，防火墙起到了类似的作用，即阻断来自外部网络的威胁和入侵，提供扼守本网络的安全和审计的关卡。防火墙技术主要依赖于两种基本准则：一是拒绝所有未经说明允许的命令，二是允许所有未经说明拒绝的命令。第一种准则提高了安全性但减弱了可用性，而第二种准则则提高了可用性但增加了安全性的难度。防火墙可以限制非法用户，如黑客和网络破坏者，进入内部网络，并禁止存在安全脆弱性的服务和

未授权的通信进出网络。防火墙有多种类型，包括过滤防火墙、应用网关防火墙、服务防火墙和监控防火墙。过滤防火墙主要工作在数据链路层和IP层，根据预设的过滤规则对数据包进行过滤。应用网关防火墙则工作在应用层，通过逻辑分析来过滤危险数据。服务防火墙主要用于服务器的保护，防止外部网络的恶意信息进入服务器的网络环境。监控防火墙不仅像传统防火墙一样过滤网络中的有害数据，还会主动对数据进行分析和测试，以发现外部攻击[2]。防火墙的功能还包括对网络存取和访问的记录、监控，作为单一的网络接入点，所有进出信息都必须通过防火墙，因此防火墙非常适合收集关于系统和网络使用和误用的信息并做出日志记录。防火墙还可以实现网络地址转换（NAT），用于缓解地址空间短缺的问题，并消除机构在变换ISP时带来的重新编址的麻烦。

3.2 入侵检测与防御系统

入侵检测和防御系统（Intrusion Detection and Prevention Systems，简称IDPS）是网络安全的重要组成部分。它们可以监视网络或系统的活动，寻找可能的恶意行为或违反策略的行为，并采取相应的措施，如发送警告、阻止活动或向其他安全设备（如防火墙）发送信号。IDPS根据其工作方式和位置可以分为网络入侵检测系统（NIDS）、主机入侵检测系统（HIDS）、网络入侵防御系统（NIPS）和主机入侵防御系统（HIPS）。NIDS监视整个网络流量，可以发现网络攻击，如拒绝服务攻击、扫描或僵尸网络。HIDS则监视单个主机，如服务器或工作站，可以发现主机级别的攻击，如恶意软件、特洛伊木马或权限提升。NIPS和HIPS不仅可以发现攻击，还可以阻止它们。IDPS的工作原理主要依赖于特征匹配和异常检测两种技术。特征匹配是通过比较网络或系统活动与已知的攻击特征（也称为签名）来发现攻击。异常检测则是通过比较网络或系统活动与正常的行为模式来发现攻击。配置IDPS涉及定义网络或系统的正常行为模式，以及选择想要检测的攻击特征。处理IDPS发现的威胁需要一些步骤，包括确认警告是否真的是攻击、分析攻击的性质和影响，以及根据分析结果采取相应的响应措施，如阻止攻击流量、清理受影响的系统或更新安全策略。

3.3 加密技术

数据加密技术是通过特定的算法将明文（未加密的数据）转换为密文（加密后的数据），使得只有拥有正确密钥的接收者才能将密文还原为明文，从而保护数据的机密性、完整性和可用性。在电子信息工程中，常见的数据加密算法主要分为对称加密算法和非对称加密算法两大类。对称加密算法，也称为单钥加密算法，其加密和解密使用相同的密钥。常见的对称加密算法有AES（高级加密标准）、DES（数据加密标准）等。AES由于其安全性高、效率快等优点，在电子信息工程中得到了广泛的应用。然而对称加密算法也存在一些不足之处，如密钥分发和管理的难题。如果密钥在传输过程中被窃取，加密的数据就会失去安全性。非对称加密算法，也称为公钥加密算法，使用一对密钥，即公钥和私钥。公钥可以公开，任何人都可以使用公钥对数据进行加密，但只有拥有私钥的人才能解密。常见的非对称加密算法有RSA算法等。在实际应用中，通常会使用非对称加密算法来交换对称加密算法的密钥，然后使用对称加密算法对大量的数据进行加密传输。这种方法结合了对称加密算法的高效性和非对称加密算法的安全性。数据加密技术在电子信息工程中的应用场景非常广泛，包括网络通信、电子商务和云计算环境等。在网络通信中，无论是有线网络还是无线网络，数据加密技术都可以防止数据在传输过程中被窃取或篡改。在电子商务中，加密技术可以保护用户的个人信息、支付信息等敏感数据，确保交易的安全进行。在云计算环境中，用户的数据存储在云端，通过加密技术可以保障数据的隐私和安全[3]。

3.4 虚拟专用网络（VPN）技术

虚拟专用网络（VPN）是在公用网络上建立专用网络的技术。VPN的主要隧道协议有PPTP、L2TP、IPSec、SSL VPN和TLS VPN。PPTP是一种用于让远程用户拨号连接到本地的ISP，通过Internet安全访问内网资源的技术。L2TP是PPTP与L2F的一种综合，由思科、微软等公司推出的一种工业标准。IPSec协议在隧道外面再封装，保证了隧道在传输过程中的安全。SSL和TLS技术是在传输层实现VPN的技术。IPSec是通过对IP协议的分组进行加密和认证来保护IP协议的网络传输协议簇。IPSec工作在TCP/IP协议栈的网络层，为TCP/IP通信提供访问控制机密性、数据源验证、抗重放、数据完整性等多种安全服务。IPSec VPN应用场景分为站点到站点、端到端和端到站点三种模式。MPLS VPN则是利用多协议标记交换技术实现的一种VPN技术。MPLS通过标签交换取代复杂的路由运算和路由交换，提高了路由器转发速率。MPLS VPN承载平台由P路由器、PE路由器和CE路由器组成，其中PE路由器负责待传送数据包的MPLS标签的生成和去除，以及发起根据路由建立交换标签的动作。

3.5 身份认证与访问控制

身份认证是确认用户身份的过程，常见的身份认证方式包括用户名和密码、指纹识别、面部识别等。访问

控制则是根据用户的身份和权限，限制其对系统资源的访问。身份认证技术确保只有合法的用户才能访问网络资源，防止了未经授权的访问和潜在的安全威胁。访问控制技术则根据用户的身份和权限，对系统资源进行细粒度的控制，确保用户只能访问其被授权的资源。身份认证和访问控制通常与其他网络安全技术结合使用，如防火墙、入侵检测系统和加密技术，以提供全面的安全防护。该企业还会通过访问控制技术限制不同用户对其交易数据的访问权限，以防止数据泄露和滥用[4]。身份认证和访问控制在保障网络安全方面发挥着至关重要的作用。通过确保只有合法的用户才能访问敏感信息和系统资源，它们有效地防止了未经授权的访问和潜在的安全威胁。与其他网络安全技术的结合使用，它们提供全面的安全防护，确保电子信息工程系统的安全性和可靠性。

4 未来电子信息工程中网络安全防护技术的发展趋势

未来电子信息工程中网络安全防护技术的发展将呈现多元化、智能化和动态化的趋势。随着人工智能技术的不断发展，其在网络安全防护领域的应用将越来越广泛。通过深度学习和机器学习，系统能够识别出潜在的网络威胁和攻击模式，实现更高效的安全防护。自动化的安全操作也将成为可能，如自动化的补丁管理系统能够根据漏洞的严重性和网络环境自动应用补丁，从而减少人为错误的风险。区块链技术因其去中心化和不可篡改的特性，正在被广泛应用于网络安全领域。通过加密算法和共识机制，区块链能够确保数据的完整性和真实性。区块链技术还可以用于身份验证，确保用户身份的真实性，减少了身份盗用的风险。智能合约作为区块链技术的一项重要应用，可以自动执行合约条款，减少人为干预的可能性，提高交易的安全性和效率[5]。零信任架构作为一种新兴的网络安全理念，也将得到广泛的推广和应用。零信任架构强调“永不信任，始终验证”，所有用户和设备都需要经过严格的身份验证和授权才能访问敏感数据和资源。这种机制能够有效降低网络风险，提高网络的安全性。零信任架构还强调网络的微分段和持续监控，以便及时发现和响应潜在的安全威胁。随着量子计算技术的不断发展，其对网络安全的影响也不容忽视，量子计算能够在极短的时间内破解传统的公钥加密算法，因此现有的加密技术需要进行更新以抵御量子计算带来的威胁。量子加密技术也应运而生，如量子密钥分发（QKD）利用量子力学的原理确保密钥的安全性，成为未来网络安全技术的重要发展方向。

结束语

综上所述，电子信息工程中的网络安全防护技术研究是一个复杂而持续的课题。面对不断演变的网络攻击手段，必须不断更新和完善防护技术，确保信息社会和谐稳定。未来，随着人工智能、区块链、量子计算等新兴技术的融入，网络安全防护将更加智能化、动态化。我们要积极探索新技术在网络安全领域的应用，为构建更加安全可靠的电子信息环境贡献力量。

参考文献

[1]李明.网络安全防护技术的发展趋势与展望[J]. 信息技术与信息化, 2022(4):89-91.

[2]张婷.主要的网络安全防护技术及其应用[J]. 计算机应用与软件, 2023(1):78-80.

[3]王琳.网络安全防护技术在信息工程中的应用研究[J]. 信息技术与信息化, 2023(5):92-94.

[4]张倩伟.面向智能时代的网络信息安全防护策略[J]. 信息安全技术学报,2023(4):150-155.

[5]李晓燕.大数据环境下的计算机网络信息安全防护研究[J].电子科技与应用,2022(3):80-86.