计算机电子信息工程技术的应用和安全

王洪志
哈尔滨惠众宜家网络科技有限公司　黑龙江　哈尔滨　150000

摘　要：计算机电子信息工程技术作为现代科技的重要支柱，其应用已广泛渗透到工业、商业及社会服务等各个领域。在工业领域，它推动了智能制造和供应链管理的革新；在商业领域，它促进电子商务和商业智能的发展；在社会服务领域，它则提升教育和医疗服务的便捷性与质量。随着技术的广泛应用，安全问题也日益凸显。确保数据的保密性、完整性和可用性，防止网络攻击和隐私泄露，已成为计算机电子信息工程技术应用中的重要挑战。

关键词：计算机；电子信息工程技术；应用；安全

1 计算机电子信息工程技术概述

计算机电子信息工程技术是一门综合性的学科，它融合了电子技术、信息技术以及计算机技术等多个领域的理论和技术。该专业主要研究如何利用这些技术来获取、传输、处理和应用信息，涉及电路设计、信号处理、通信技术和计算机科学等多个方面。在计算机电子信息工程技术中，学生需要掌握电子技术、信号处理、通信原理、计算机网络、传感器与检测技术、嵌入式系统等方面的基本理论和技能。这些技能使得毕业生能够在通信、电子设备制造、物联网、智能制造等多个领域发挥自己的专业知识和技能[1]。随着5G、人工智能、物联网等新兴技术的不断发展，计算机电子信息工程技术正朝着智能化、网络化和集成化的方向发展。这些新技术将进一步推动电子信息工程迈向更高的高度，智能设备、智能家居、智慧城市等将成为现实。

2 计算机电子信息工程技术应用中的安全问题

2.1 网络攻击与黑客入侵

在计算机电子信息工程技术的应用中，网络攻击与黑客入侵是首要的安全威胁。黑客可能通过各种手段，如网络钓鱼、拒绝服务攻击、密码破解等，试图非法访问或破坏系统。这些攻击不仅可能导致系统瘫痪，还可能造成敏感信息的泄露，给企业和个人带来巨大损失。

2.2 数据泄露与隐私侵犯

数据泄露与隐私侵犯是电子信息工程中的另一大安全问题。随着大数据时代的到来，个人信息和敏感数据的安全问题日益凸显。如果数据库的安全防护措施不到位，黑客可能轻易入侵并窃取数据。一些企业和机构在未经用户授权的情况下，将用户数据用于其他商业目的或与第三方共享，也严重侵犯了用户的隐私权。

2.3 系统故障与数据丢失

系统故障与数据丢失是电子信息工程应用中不可忽视的安全问题。硬件故障、软件故障和网络故障都可能导致系统崩溃或数据丢失。这些故障不仅会影响系统的正常运行，还可能造成无法挽回的数据损失。

2.4 恶意软件与病毒传播

恶意软件与病毒传播是电子信息工程中的常见安全问题。计算机病毒、木马、蠕虫等恶意软件能够自我复制并传播到其他计算机系统，对系统进行破坏或窃取信息。这些恶意软件的传播方式多样，如通过邮件附件、不可信网站下载的软件包、可移动存储设备等[2]。

3 计算机电子信息工程技术的安全防护措施

3.1 防火墙与入侵检测系统

在计算机电子信息工程技术的安全防护措施中，防火墙与入侵检测系统（IDS）构成了重要的第一道和第二道防线。防火墙是一种网络安全设备或系统，其主要功能是根据预定的安全规则监控和控制网络流量，以保护网络免受未经授权的访问和攻击。它通过流量过滤、访问控制、网络地址转换（NAT）以及日志记录与审计等多种机制，有效地阻止恶意流量，保护内部网络免受外部威胁。防火墙可以按照其实现方式和工作层次进行分类，主要包括包过滤防火墙、代理防火墙、状态检测防火墙和下一代防火墙。包过滤防火墙基于OSI模型的网络层，对每个数据包的源地址、目的地址、端口等进行检查，决定是否允许其通过，但无法理解应用层的数据，容易被复杂攻击绕过。代理防火墙则通过代理服务器接收请求，再将请求转发到目标服务器，能够理解应用层协议，如HTTP、FTP等，但可能消耗较多的处理资源，影响网络性能。状态检测防火墙监控数据包的状态，跟踪连接的每个状态，并根据连接状态动态创建规则来允许或拒绝数据包，结合了包过滤和应用层检查的优点，但复杂度较高，对硬件性能要求较大。而下一代防火墙结合了状态检测、防病毒、入侵检测等功能，能够深入

理解应用层数据流，提供更全面的防护，但价格昂贵，配置和管理复杂。入侵检测系统（IDS）则是一种用于监控网络或系统活动，以检测潜在的安全威胁和攻击的设备或软件。IDS与防火墙的主要区别在于，防火墙用于阻止攻击，而IDS用于检测和告警。IDS通过分析网络流量和系统日志，寻找已知攻击模式或异常行为。如果检测到可能的攻击，IDS会向管理员发出警报，以便采取相应措施。基于网络的IDS（NIDS）部署在网络的关键节点，分析网络流量，以检测攻击行为，但无法检测加密流量中的攻击。基于主机的IDS（HIDS）则部署在特定的主机上，分析系统日志和文件的变化，以检测攻击，但无法看到主机外的网络流量。

3.2 数据加密与身份认证技术

数据加密与身份认证技术是计算机电子信息工程技术安全防护的重要措施。数据加密技术通过将原始数据转换为一种不易被理解的形式，从而实现对数据的保密性和防止非法访问。常见的网络数据加密技术包括对称加密和非对称加密。对称加密使用同一个密钥对数据进行加密和解密，加密效率高，但密钥的传输和管理比较困难，容易被攻击者获取密钥。非对称加密则使用一对密钥，公钥和私钥进行加密和解密，密钥的传输不需要保密，但加密和解密的效率相对较低[3]。常见的非对称加密算法包括RSA和椭圆曲线加密算法。身份认证技术用于验证用户的身份，确保只有经过授权的用户才能访问特定的资源。常见的身份认证技术包括密码认证、多因素认证和生物特征认证。密码认证是最常见也是最基础的身份认证技术，用户通过输入正确的用户名和密码进行身份验证，但容易被猜解和攻击。为了提高密码认证的安全性，用户应当选择强密码，并定期更改密码。多因素认证结合了多个身份认证因素，如密码、指纹、声纹等，用户需要提供两个或多个因素进行身份验证，这种方式可以提高安全性，防止密码被盗用或破解。生物特征认证则使用个体的生物特征作为身份认证的依据，如指纹、虹膜、声纹等，生物特征是每个人独一无二的，因此该认证方式较为安全，但设备成本较高，且可能对隐私造成一定程度的侵犯。数据加密与身份认证技术的结合使用，可以确保数据的机密性和完整性，防止数据泄露和隐私侵犯，为计算机电子信息工程技术的安全提供有力的保障。

3.3 漏洞扫描与修复

漏洞扫描与修复是计算机电子信息工程技术安全防护的重要环节。了解并识别安全漏洞类型，是制定有效安全防护措施的前提。这包括但不限于跨站脚本攻击（XSS）、跨站请求伪造（CSRF）、点击劫持、SQL注入、远程代码执行（RCE）等。选用合适的漏洞扫描工具，如OWASP ZAP、Burp Suite、Netsparker等专业安全扫描工具，能够帮助自动检测各种安全漏洞。它们能深入扫描应用接口、网页和其他网络资源，输出详尽的漏洞报告。在DevOps实践中，应将安全漏洞扫描工具集成到持续集成/持续部署（CI/CD）管道中，确保每次代码变更时都能自动进行安全扫描。用户输入验证与过滤也是防止漏洞被利用的关键措施。在接收和处理用户输入时，务必进行严格的验证和过滤，使用白名单或黑名单模式限制输入内容，防止恶意脚本注入等攻击。对于发现的漏洞，应及时进行分析和分类，并按照漏洞的严重性、影响范围和利用难度等因素进行优先级排序。一般来说，高危漏洞应当优先得到修复。为每个漏洞制定具体的修复步骤、目标时间表和所需的资源分配，对于某些已知的、标准化的低复杂度漏洞，可以考虑使用自动化脚本或工具进行修复，以提升效率和一致性。修复漏洞后，通过漏洞扫描工具再次扫描以确认漏洞已被消除，并使用网络监测工具对网络系统进行持续监控，确保系统在修复后仍保持稳定安全。设置定期的全网安全扫描，跟踪最新的安全漏洞公告，并及时响应新的安全威胁，不断完善和更新安全策略及修复程序。通过漏洞扫描与修复，可以及时发现并修补系统中的安全漏洞，降低被黑客利用的风险，提高计算机电子信息工程技术的安全防护能力。

3.4 网络安全态势感知

网络安全态势感知是计算机电子信息工程技术安全防护的高级阶段。态势感知一词来源于对抗行动和战争，进入信息化时代后，作战形态发生改变，不断向虚拟的网络空间延伸，网络安全态势感知的概念由此形成。所谓“知己知彼百战不殆”，网络安全态势感知即是在大规模网络环境中，对能够引起网络态势发生变化的安全要素进行获取、理解、显示并据此预测未来的网络安全发展趋势。网络安全态势感知涉及多个关键技术，包括数据采集、态势理解、态势评估、态势预测和态势可视化等[4]。数据采集是态势感知的第一步，使用软件和硬件技术对各种影响网络系统安全的数据进行采集，包括资产数据、威胁数据、漏洞数据、脆弱性数据、用户异常行为数据、网络服务数据等。态势理解是对海量数据进行分类、归纳和关联分析，得出影响网络的整体安全状况。态势评估则需要结合多个数据维度，划分各种影响要素，进行定性、定量分析，评估网络当前的安全状态和薄弱环节，并给出相应的应对措施。态

势预测则是通过过去和当前已知安全要素，预测将来影响网络安全事件因素的变化规律，进而提前预测网络安全状况的发展趋势。态势可视化则利用可视化技术，以地图、表格、树状图、时间轴、3D和层次可视化等形式展示网络安全态势状况，帮助用户更直观、准确地理解网络安全整体态势。通过网络安全态势感知，可以实时掌握网络系统的安全状况，及时发现并应对潜在的安全威胁，提高安全防护的主动性和预见性。网络安全态势感知还可以为网络安全策略的制定和优化提供数据支持，推动安全防护体系的不断完善和升级。

4 计算机电子信息工程技术的应用

4.1 工业领域

在计算机电子信息工程技术的众多应用中，工业领域无疑是一个重要且广泛的领域。随着工业4.0时代的到来，计算机电子信息工程技术为传统工业带来了前所未有的变革。在智能制造方面，通过集成物联网、大数据、云计算等先进技术，实现了生产过程的自动化、智能化和高效化。智能设备能够实时监测生产数据，进行精准控制，提高生产效率和产品质量。计算机电子信息工程技术还促进工业机器人的广泛应用，这些机器人能够执行复杂、精细的操作，减轻工人的劳动强度，提高生产安全性。在供应链管理、能源管理、环境监测等方面，计算机电子信息工程技术也发挥着重要作用，推动工业领域的可持续发展。

4.2 商业领域

商业领域是计算机电子信息工程技术的又一重要应用领域。在电子商务方面，通过构建在线交易平台，实现商品信息的快速传递和交易过程的便捷化。消费者可以随时随地浏览商品信息、下单购买，而商家则可以通过数据分析了解消费者需求，优化产品设计和营销策略[5]。计算机电子信息工程技术还促进了商业智能的发展，通过数据挖掘和分析，企业可以获取有价值的市场信息，为决策提供支持。在客户关系管理方面，通过集成CRM系统，企业可以更有效地管理客户信息，提高客户满意度和忠诚度。计算机电子信息工程技术还为金融行业提供了安全、高效的交易平台和支付系统，推动了金融业务的创新和发展。

4.3 社会服务领域

社会服务领域也是计算机电子信息工程技术的重要应用场所。在教育领域，通过在线教育平台，人们可以随时随地接受优质教育资源，打破了地域和时间的限制。计算机电子信息工程技术还为教育提供了丰富的多媒体教学资源，提高了教学效果和学习体验。在医疗领域，通过电子病历系统、远程医疗等应用，患者可以获得更加便捷、高效的医疗服务。医生可以远程为患者提供诊断和治疗建议，而患者则可以通过电子病历系统方便地查看自己的健康状况和医疗记录，计算机电子信息工程技术还在交通、公共安全、环境保护等领域发挥着重要作用，推动了社会服务领域的智能化和便捷化发展。

结束语

综上所述，计算机电子信息工程技术的应用为各行各业带来了前所未有的变革与机遇，但同时也伴随着严峻的安全挑战。未来，随着技术的不断进步和应用的深化，需要持续加强安全防护措施，提升系统的安全性和可靠性。只有这样，才能确保计算机电子信息工程技术在推动社会进步的同时，也为人们提供一个安全、可信的数字环境。

参考文献

[1]张超.电子信息工程中的计算机技术应用及其安全研究[J].电子元器件与信息技术,2020,4(07):14-15.

[2]赵凯.计算机电子信息工程技术的应用与安全探讨[J].信息系统工程,2020(05):68-69.

[3]王蕾.计算机电子信息工程技术的应用与安全探讨[J].电脑编程技巧与维护,2020(02):158-160.

[4]金雷.计算机电子信息工程技术的应用和安全管理分析[J].计算机产品与流通,2020(03):66.

[5]宋美霖.计算机电子信息工程技术的应用和安全问题分析[J].信息系统工程,2020(04):62-63.