电子信息工程中的安全技术应用分析

柳明君
栖霞市消费者投诉中心

摘　要：信息技术不断创新发展，在诸多行业领域得到了广泛应用，相应的也对人们日常生产生活产生了巨大的影响。也正是由于信息技术的广泛应用，电子信息工程规模进一步扩大，信息安全问题相伴随而来，如何保证信息安全则成为社会各界重点关注的内容。因此，为了推动电子信息工程高水平发展，选择切实可行的安全技术是尤为必要的，以求将安全隐患消灭在萌芽状态。本文就电子信息工程中安全技术的实际应用内容进行分析，为安全技术大范围推广应用提供支持。

关键词：安全技术；电子信息工程；传感技术；数据加密；网络防火墙

【DOI】10.12254/j.issn.2096-6539.2023.11.088

前言

随着信息技术的迅猛发展和广泛应用，电子信息工程在各个领域中扮演着至关重要的角色。然而，随之而来的是信息安全面临的巨大挑战。不断涌现的网络攻击、数据泄漏以及恶意软件等威胁，给个人、组织和整个社会带来了巨大的风险。因此，安全技术在电子信息工程中的应用分析显得尤为重要。安全技术在电子信息工程中扮演着保护和维护信息系统安全的关键角色，它涵盖了一系列方法、技巧和工具，有助于识别、预防和应对各种安全威胁。关于电子信息工程中安全技术的应用分析，旨在提升电子信息工程的安全性，更好的抵御潜在安全风险。

一、电子信息工程的应用表现

（一）电子信息工程概述

电子信息工程是一门综合性的学科，涵盖了电子技术、通信技术和计算机技术等多个领域。它致力于研究和应用电子设备、通信系统和信息处理技术，以满足人们对信息获取、处理和传输的需求[1]。

在当今信息化时代，电子信息工程在各个领域中发挥着重要的作用。无论是通信、互联网、医疗、交通还是工业控制等领域，都离不开电子信息工程的支持和应用。它的发展推动了信息技术的进步，极大地改变了人们的生活方式和工作方式。电子信息工程的核心是信息的获取、处理和传输。通过电子设备和通信系统，可以采集、传输和存储大量的数据和信息[2]。电子信息工程涉及传感器、信号处理、通信协议、网络技术、数据库管理等多个方面的知识和技术。然而，随着信息技术的广泛应用，信息安全问题变得尤为重要。电子信息工程中的数据和信息需要受到保护，以防止未经授权的访问、篡改、泄漏或破坏。因此，安全技术在电子信息工程中具有重要的地位和作用。

（二）电子信息工程技术的应用表现

（1）传感技术。传感技术在电子信息工程中扮演着重要的角色。通过传感器，电子信息工程可以获取各种物理量、环境参数和生物特征等数据。这些传感器可以广泛应用于安防系统、智能家居、工业自动化等领域[3]。在安全技术方面，传感技术的应用可以实时监测和检测安全事件，如入侵检测、火灾报警等。传感技术与安全技术的结合可以提高信息系统的实时感知和响应能力。

（2）物联网技术。物联网技术是将各种设备和物体连接到互联网，并实现互相通信和交互的技术[4]。在电子信息工程中，物联网技术的应用非常广泛。通过物联网技术，安全设备、智能家居设备、车辆、工业设备等可以互相连接，并实现远程监控、数据共享和智能控制。在安全技术方面，物联网技术可以实现对安全设备和系统的远程监控和控制，提高安全性和便捷性。例如，通过物联网技术，可以远程监控家庭安防系统，并实时获取安全事件的警报和图像信息。

（3）信息集成技术。信息集成技术是指将来自不同来源的信息进行整合和融合的技术。在电子信息工程中，信息集成技术可以将来自各种传感器、数据库、云平台等的信息进行集成，形成全面的信息视图。在安全技术方面，信息集成技术可以实现多源数据的整合和分析，帮助识别和评估安全威胁。例如，将来自视频监控、访问日志、入侵检测系统等的信息进行集成分析，可以更准确地判断是否存在安全风险[5]。

三、电子信息工程中的安全问题分析

（一）黑客攻击

在电子信息工程中，黑客攻击是一种常见的安全问题。黑客指的是具有高级计算机技术的人员，他们试图未经授权地获取、修改、破坏或篡改信息系统中的数据和资源。

黑客攻击的形式多种多样，包括但不限于以下几种：

（1）网络入侵。黑客通过攻击网络设备、操作系统漏洞、应用程序漏洞等方式，非法进入目标系统。他们可能利用恶意软件、网络钓鱼、拒绝服务攻击等手段，窃取敏感信息或破坏系统的正常运行[6]。

（2）数据泄漏。黑客通过攻击数据库、文件共享系统等，获取系统中的敏感数据，并将其公之于众。这种攻击可能导致个人隐私泄漏、商业机密被窃取等严重后果。

（3）社会工程学攻击。黑客可能利用社会工程学技巧，通过欺骗、诱导、伪装等手段，获取系统的访问权限。他们可以冒充合法用户，从内部进行攻击或者获取敏感信息。

（4）漏洞利用。黑客利用尚未被发现或公开的漏洞，通过针对性的攻击手段，入侵系统并进行恶意活动。这种攻击方式尤为危险，因为受害者往往没有相应的防御措施[7]。

（二）计算机病毒

计算机病毒是一种恶意软件，它通过在计算机系统中复制和传播自身来感染系统，并可能破坏、删除或篡改数据，甚至使系统完全无法正常工作。计算机病毒的传播和入侵途径主要有以下几种。

（1）恶意附件、病毒通过电子邮件、即时消息等途径传播，常伴随着伪装成正常文件或链接的恶意附件。一旦用户打开或下载这些附件，病毒便会感染系统。

（2）感染式病毒。感染式病毒会将自身代码嵌入到可执行文件或系统文件中，当用户执行这些文件时，病毒会感染其他文件并传播到其他系统。

（3）网络传播。病毒可以通过网络漏洞或未经授权的远程访问，利用系统中的弱点远程传播和感染其他计算机。

（4）可移动介质。病毒可以通过可移动介质，如USB闪存驱动器、移动硬盘等，传播到其他计算机[8]。

（三）数据泄漏

数据泄漏是电子信息工程中极为敏感和严重的安全问题。当系统中的敏感数据被非法访问或泄漏，将导致个人隐私曝光、商业机密泄漏等严重后果[9]。数据泄漏可能是由黑客攻击、内部人员不当操作、不安全的数据存储等原因引起。

（四）身份认证与访问控制

在电子信息工程中，确保用户的身份认证和访问控制是关键的安全问题。如果未经授权的用户获得了系统的访问权限，将可能导致数据泄漏、系统被篡改等问题。因此，建立有效的身份认证和访问控制机制，限制和管理用户的权限和访问权限至关重要。

除了网络和数据安全外，电子信息工程还需要关注物理安全问题。物理设备和设施的安全性直接影响到整个系统的安全。例如，防止设备被盗、丢失或未经授权的物理访问，以及建立安全的数据中心和机房等都是物理安全的重要方面。

四、电子信息工程中的安全技术的实践应用

安全技术是指应用于电子信息工程中，以保护信息系统安全的技术手段和方法。它涵盖了识别和评估安全威胁、设计和实施安全策略、建立安全控制措施、监测和应对安全事件等方面的内容。安全技术的应用可以有效地保护信息系统的机密性、完整性和可用性，确保信息的安全传输和存储。

（一）数据加密处理

在电子信息工程中，数据加密是一项常见且关键的安全技术。数据加密是指通过使用密码算法将敏感数据转换为密文，以保护数据的机密性和完整性，防止未经授权的访问和篡改。在网络通信中，数据经常需要通过不安全的通道传输，如公共网络或无线网络。为了保护数据的机密性，通信双方可以使用加密算法对数据进行加密。加密后的数据只能被授权的接收方解密并还原为明文。在电子信息系统中，大量的数据需要进行存储，包括用户个人信息、商业机密等敏感数据。为了防止数据泄漏或被非法访问，可以使用数据加密技术对数据进行加密存储[10]。即使存储介质被盗或遭到物理访问，未经授权的人员无法解密和获取数据。在电子信息工程中，身份认证是确保系统安全的重要环节。数据加密技术可以用于用户身份认证过程中的敏感信息保护。例如，使用加密技术对用户密码进行加密存储，防止密码泄漏后被恶意利用。在数字内容传播和分发过程中，数据加密可以用于保护版权和防止盗版。通过对数字内容进行加密，只有具备合法许可的用户才能解密并使用内容，从而保护版权和控制内容的合法使用。

为实现数据加密的实践应用，电子信息工程中采用了多种加密算法和技术，如对称加密算法、非对称加密算法和哈希函数等。同时，还需要合理的密钥管理和安全协议设计，确保加密过程的安全性和可靠性。

（二）建设和完善网络防火墙

在电子信息工程中，网络防火墙是一项关键的安全技术，用于保护网络系统免受未经授权的访问、恶意攻击和网络威胁的侵害。网络防火墙通过监测、过滤和控制网络流量，实现对进出网络的数据包进行检查和管理，从而确保网络的安全性和稳定性。

就网络防火墙在电子信息工程中应用情况来看，主要表现在以下几点：①访问控制：网络防火墙可以通过访问控制策略，限制对网络资源和服务的访问权限。它可以定义规则，只允许经过授权的用户或特定IP地址访问网络，阻止未经授权的访问和潜在的攻击者。②流量过滤：网络防火墙能够检测和过滤网络流量中的恶意数据包和攻击尝试[11]。它可以通过深度包检测、状态检查和内容过滤等技术，识别和阻止传入和传出网络的恶意流量，如病毒、蠕虫、DoS攻击等。③VPN安全：虚拟专用网络（VPN）是远程访问和安全通信的重要方式。网络防火墙可以支持建立安全的VPN连接，对通过公共网络传输的数据进行加密和隧道封装，确保远程用户和分支机构的安全通信。④日志记录与审计：网络防火墙可以记录和存储网络流量、安全事件和用户活动的日志信息。这些日志记录可以用于安全事件的追踪和分析，帮助发现潜在的安全威胁和入侵行为，及时采取相应的应对措施。⑤远程访问管理：网络防火墙还可以用于管理远程访问，包括远程管理和远程桌面等功能。它可以限制和监控远程访问的权限和行为，减少远程攻击和未经

授权的访问风险。由此看来，网络防火墙的实际应用，要选择合理技术，合理设计网络拓扑和规则策略，定期进行安全评估和漏洞扫描，并及时更新防火墙规则和软件补丁，以保证网络防火墙的有效性和可靠性。

（三）推行身份信息验证

身份信息验证是确认用户身份和授权访问的过程，旨在防止未经授权的用户获取系统资源和敏感信息，确保系统的安全性和可信度。电子信息系统通常要求用户通过登录认证来访问系统资源，身份信息验证技术可用于验证用户的身份和凭据，如用户名和密码、数字证书、生物特征识别等。只有成功验证身份的用户才能获得访问权限。为提高身份验证的安全性，电子信息工程中推行多因素认证。多因素认证要求用户提供多个身份验证要素，如密码和指纹、密码和动态验证码等。这样可以提高身份验证的可靠性，降低被破解或冒用的风险[12]。

一般情况下，在大型电子信息系统中，用户通常需要登录多个应用和服务。单一登录技术允许用户只需进行一次身份验证，即可访问多个应用和服务，减少了重复登录的繁琐，同时提供了集中的身份管理和控制。电子信息工程中的身份信息验证需要使用安全的身份认证协议，如，使用安全的身份认证协议如OAuth、OpenID Connect等来实现用户的安全认证和授权，确保用户身份信息的安全传输和处理。除此之外，身份信息验证也用于强化访问控制，通过验证用户的身份，可以根据其权限和角色来限制和管理对系统资源的访问。只有经过身份验证且具备相应权限的用户才能进行特定操作和访问敏感信息。

（四）建立安全性较高的网络平台

网络平台是指用于提供各种服务和资源的网络基础设施，如云计算平台、物联网平台、电子商务平台等。确保网络平台的安全性对于保护用户数据、防止恶意攻击和确保系统可用性至关重要。在建立网络平台时，应考虑安全性的设计和架构。这包括采用分层架构、隔离不同功能模块、实现数据加密和传输的安全协议，以及使用安全硬件模块和安全算法等，确保平台的安全性和可靠性。网络平台中的漏洞可能被黑客利用来进行攻击，对此需要建立漏洞管理和修补机制，定期对平台进行漏洞扫描和安全评估，及时修补已发现的漏洞，减少被攻击的风险。网络平台应实施安全的访问控制策略，确保只有经过授权的用户和设备才能访问平台。这包括用户身份验证、权限管理、访问日志记录和审计等措施，限制非法访问和提供行为的监控。更为关键的是，为了灵活应对突发安全事件，应建立安全监测和响应机制，及时检测和应对安全事件。通过使用入侵检测系统、安全信息和事件管理系统等工具，实时监测网络平台的安全状况，发现异常行为和攻击，采取相应的应对措施。

（五）合理化运用入侵检测技术

入侵检测技术旨在通过监控和分析网络流量、系统日志和行为模式等，及时发现和响应潜在的入侵活动，以保护系统免受未经授权的访问和恶意攻击。通过在网络中部署网络入侵检测系统，监控网络流量并识别异常和恶意行为。NIDS可以检测诸如端口扫描、DDoS攻击、恶意软件传播等常见的网络入侵活动，并及时发出警报或采取阻断措施。在主机上部署主机入侵检测系统，监测主机的操作系统、应用程序和文件系统等，以侦测主机上的异常行为和潜在的入侵活动。HIDS可以检测到未经授权的文件修改、异常进程行为、恶意代码执行等情况。

结论

总的说来，电子信息工程快速发展，在带来了巨大的经济效益同时，却也面临着不同程度的安全挑战。为了推动电子信息工程良性发展，积极引用安全技术是至关重要的，有助于抵御不安全的入侵行为，最大程度上保障信息安全。

参考文献

[1]袁娜.浅析计算机网络技术在电子信息工程中的实践[J].科技资讯，2017，15（19）：33-34.

[2]刘彦凯.关于电子信息工程中的计算机技术应用及安全的思考[J].信息系统工程，2021（10）：62-64.

[3]袁晓明.电子信息工程技术的应用及安全管理探究[J].现代盐化工，2020，47（06）：179-180.

[4]张璐明.电子信息工程技术的应用与安全防护研究[J].电子技术与软件工程，2020（21）：257-258.

[5]张立站.探究计算机电子信息工程技术的应用及安全[J].数码世界，2020（11）：38-39.

[6]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.

[7]孙维玖.关于计算机电子信息工程技术的应用实现及安全管理探讨[J].计算机产品与流通，2020（08）：118.

[8]樊旗.分析新时期下的计算机电子信息工程技术的安全与应用[J].数字技术与应用，2020，38（04）：192-193.

[9]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.

[10]徐赟.计算机网络技术在电子信息工程中的实践创新[J].产业与科技论坛，2020，19（01）：66-67.

[11]齐邦强.信息安全技术在电子信息工程中的应用与解析[J].信息与电脑（理论版），2019，31（19）：197-198+201.

[12]赵炳会.关于计算机电子信息工程技术的应用实现及安全管理探讨[J].电子制作，2018（16）：49-50+35.