

计算机网络安全防护技术探析

孟思李尧

河北省桃林口水库事务中心 河北 秦皇岛 066000

摘要: 计算机网络安全是确保网络环境中的数据保密性、完整性及可使用性免受破坏的关键领域。本文概述了网络安全的主要威胁、影响因素,并探讨了防火墙技术、数据加密技术、访问控制技术、防御病毒技术以及入侵检测技术等关键防护技术。同时,提出了综合运用安全防护技术、加强安全管理和监控、提高用户安全意识及建立应急响应机制等策略,以全面保障计算机网络安全。

关键词: 计算机网络;安全防护技术;防护策略

引言:随着信息技术的迅猛发展,网络已成为现代社会不可或缺的基础设施。然而,网络攻击事件频发,给个人、企业乃至国家带来了巨大的安全威胁。因此,深入探讨计算机网络安全防护技术,构建坚固的网络安全防线,已成为当务之急。本文旨在分析当前网络安全面临的挑战,探讨有效的防护策略和技术手段,为网络安全防护提供参考和借鉴。

1 计算机网络安全概述

1.1 计算机网络安全的定义

计算机网络安全是指利用网络管理控制和技术措施,确保在一个网络环境中,数据的保密性、完整性及可使用性受到保护。这涉及到硬件、软件、数据资源以及网络服务的全面防护,防止其因偶然或恶意的原因而遭到破坏、更改或泄露,确保网络系统能够连续、可靠地运行,网络服务正常有序。

1.2 网络安全的主要威胁类型

网络安全面临的主要威胁包括病毒、黑客攻击和恶意软件等。病毒是一种能够自我复制并感染计算机系统或网络的恶意代码,通过破坏数据、占用系统资源或传播给其他系统来造成影响。黑客攻击则是指未经授权的访问或破坏行为,黑客可能利用系统漏洞或社会工程学手段,意图窃取敏感信息、篡改数据或造成系统瘫痪。恶意软件包括但不限于间谍软件、勒索软件和挖矿软件等,这些软件未经用户同意即在用户设备上运行,进行非法的信息收集、系统控制或资源消耗等。

1.3 网络安全问题的现状和发展趋势

当前,网络安全问题日益严重,全球范围内频繁发生网络攻击事件,政府、能源、航空、金融等关键领域均面临严重威胁。这些攻击不仅造成巨大的经济损失,还影响了社会稳定和国家安全。此外,随着物联网、人工智能等新兴技术的快速发展,网络安全问题呈现出更

加复杂和多样化的特点。未来,人工智能安全技术将成为研究焦点,网络安全基础设施和公共安全服务属性将得到加强。同时,勒索软件攻击、供应链安全、隐私计算等也将继续成为网络安全领域的重点关注对象。此外,随着全球地缘政治紧张局势的加剧,国家支持的网络攻击活动正威胁到全球关键基础设施的稳定性,网络安全问题已成为各国需要共同面对的挑战。

2 计算机网络安全的影响因素

2.1 网络系统本身存在的问题

网络系统本身的设计缺陷、技术局限以及配置不当都是影响网络安全的重要因素。例如,操作系统的漏洞、应用程序的bug、协议设计中的安全缺陷等,都可能为攻击者提供可乘之机。此外,随着技术的不断发展,新的网络安全威胁不断出现,而网络系统的更新升级往往滞后于这些威胁的演变,导致系统存在潜在的安全风险。

2.2 来自外界的威胁因素

外界的威胁因素主要包括黑客攻击、恶意软件、钓鱼网站等。黑客通过利用系统漏洞、社交工程等手段,试图非法访问或破坏网络系统,窃取敏感信息或制造混乱。恶意软件如病毒、木马、勒索软件等,能够感染用户的计算机系统,窃取信息、控制设备或勒索金钱。钓鱼网站则通过伪装成正规网站,诱导用户输入个人信息,进而实施诈骗或身份盗用。

2.3 计算机用户带来的威胁因素

计算机用户的安全意识和操作习惯对网络安全具有重要影响。安全意识不足的用户容易成为网络诈骗的受害者,如点击不明链接、下载未知附件等,导致恶意软件感染或个人信息泄露。此外,不当的操作习惯,如弱密码、密码复用、共享账户等,也会增加网络系统的安全风险,用户的疏忽和无知往往成为攻击者突破系统防线的关键^[1]。

2.4 有效评估和监控手段的缺乏

有效的安全评估和监控手段是及时发现和应对网络安全威胁的重要保障。然而,许多网络系统在设计 and 运行过程中,往往缺乏全面的安全评估和持续的监控能力。这导致系统漏洞无法及时发现和修复,异常行为无法及时察觉和应对。缺乏有效的安全评估和监控手段,将使网络系统暴露在潜在的安全风险之下,增加遭受攻击的可能性。

3 计算机网络安全防护技术

3.1 防火墙技术

(1) 防火墙的定义和功能。防火墙是一种用于保护计算机网络安全系统,通过在内部网络和外部网络之间设置一道屏障,来监控和控制网络通信,以防止未授权的访问和数据泄露。防火墙能够过滤掉不安全的网络流量,只允许符合安全策略的通信通过,从而有效地保护内部网络资源。(2) 防火墙的种类。1) 包过滤型防火墙:基于网络层的数据包头信息进行过滤,通过检查源地址、目标地址、端口号等来判断数据包是否允许通过。这种方法简单高效,但缺乏上下文信息,容易被攻击者绕过。2) 应用代理网关型防火墙:在应用层对网络流量进行代理和转发,通过检查通信内容来确保安全。它能够理解并处理各种应用协议,提供更高的安全性,但性能相对较差。3) 状态检查型防火墙:结合了包过滤和应用代理的优点,通过检查数据包的上下文信息(如会话状态)来做出决策。它不仅能够过滤网络流量,还能够跟踪会话的完整性和合法性。(3) 防火墙的部署和配置策略。防火墙的部署位置通常在网络的边界处,以监控和控制进出网络的流量。根据业务需求和安全策略,可以配置访问控制列表(ACL)来定义允许或拒绝的网络流量。此外,还可以通过配置端口映射和NAT(网络地址转换)等功能,来增加网络的安全性和灵活性^[2]。

3.2 数据加密技术

(1) 数据加密的基本概念。数据加密是通过特定的算法将原始数据(明文)转换为不可读的格式(密文),以防止未经授权的访问和篡改。只有拥有相应密钥的用户才能将密文解密为明文。(2) 对称加密算法和非对称加密算法。1) 对称加密算法:使用相同的密钥进行加密和解密。常见的对称加密算法包括AES、DES等。2) 非对称加密算法:使用一对密钥(公钥和私钥)进行加密和解密。公钥用于加密数据,私钥用于解密数据。常见的非对称加密算法包括RSA、ECC等。(3) 数据加密技术的应用。数据加密技术广泛应用于网络通信安全、数据存储安全等领域。例如,SSL/TLS协议通过加

密用户和服务器之间的通信,保护数据的机密性和完整性;数字签名技术通过非对称加密算法验证数据的完整性和来源的真实性;报文摘要技术通过哈希算法生成数据的唯一标识,用于检测数据的完整性。

3.3 访问控制技术

(1) 访问控制的定义和目的。访问控制是一种通过限制对计算机系统、网络资源和数据的访问,来确保资源的安全性和保密性的技术手段。其目的是防止未经授权的用户访问敏感信息或执行未经授权的操作。(2) 访问控制模型。1) 自主访问控制(DAC):由资源的所有者决定谁可以访问该资源以及具有哪些权限。2) 强制访问控制(MAC):系统根据预先设定的安全策略,强制决定用户或进程的访问权限。3) 基于角色的访问控制(RBAC):通过为用户分配角色,然后根据角色分配权限,简化了权限管理过程。(3) 访问控制的安全策略和安全级别。访问控制的安全策略包括最小权限原则、职责分离原则等。最小权限原则要求每个用户或进程只拥有完成其任务所需的最小权限;职责分离原则要求将不同的职责分配给不同的用户或进程,以防止滥用权限。根据业务需求和安全需求,可以设定不同的安全级别,如机密级、秘密级、内部使用级等。

3.4 防御病毒技术

(1) 病毒的定义和特性。病毒是一种能够自我复制并感染计算机系统或网络的恶意代码。它通常通过网络传播,如电子邮件、文件共享等方式。病毒能够破坏数据、占用系统资源、传播给其他系统等,对网络安全构成严重威胁。(2) 防病毒技术的种类。1) 预防技术:通过实时监控和检测网络流量和系统行为,及时发现并阻止病毒的传播和感染。2) 检测技术:通过扫描文件系统、内存和网络流量等,检测并识别病毒的存在。3) 消除技术:一旦检测到病毒,采取相应措施将其从系统中清除,恢复系统的正常运行。(3) 防病毒软件的部署和更新策略。防病毒软件是防御病毒的重要手段之一。它通常部署在客户端和服务端,通过实时监控和扫描来保护系统免受病毒的侵害。为了保持防病毒软件的有效性,需要定期更新其病毒库和扫描引擎,以及配置合理的安全策略。

3.5 入侵检测技术

(1) 入侵检测的定义和目的。入侵检测是一种通过监控和分析网络流量和系统行为,及时发现并报告可疑活动的技术手段。其目的是帮助系统管理员快速响应并处理安全事件,减少损失。(2) 入侵检测系统的分类。1) 基于主机的入侵检测系统(HIDS):部署在主机上,

通过监控主机的日志文件和系统调用等信息，发现可疑行为。2) 基于网络的入侵检测系统 (NIDS)：部署在网络的关键节点上，通过监控网络流量来发现可疑的网络活动。(3) 入侵检测系统的部署和配置策略。入侵检测系统的部署位置通常根据业务需求和安全策略来确定。常见的部署方式包括边界部署、内部部署和混合部署等。配置策略包括设置合理的阈值、报警方式和响应措施等。通过定期测试和更新入侵检测系统，可以保持其有效性和准确性。

4 计算机网络安全防护策略

4.1 综合运用多种安全防护技术

计算机网络安全防护的核心在于技术的综合运用。这包括但不限于防火墙技术、数据加密技术、入侵检测与防御系统、身份认证与授权机制等。防火墙作为第一道防线，能够有效阻止未经授权的访问和数据泄露；数据加密则确保了数据的机密性和完整性，即便在数据传输过程中被截获，也无法被轻易解读；入侵检测系统能够实时监控网络异常行为，及时发现并响应潜在的安全威胁；而身份认证与授权机制则确保了只有经过验证的合法用户才能访问特定资源。此外，随着技术的不断进步，新兴的安全防护技术如人工智能安全分析、区块链数据保护等也逐渐崭露头角，为网络安全防护提供了新的思路和手段。企业应紧跟技术潮流，不断探索和实践新技术在网络安全防护中的应用，以提升整体安全防护水平。

4.2 加强网络安全管理和监控

网络安全管理是确保网络安全的重要基石。企业应建立健全的网络安全管理制度，明确各级人员的安全职责和操作规范，确保每一项网络安全措施都能得到有效执行。同时，加强网络安全监控也是必不可少的，通过对网络流量、系统日志等进行实时监控和分析，能够及时发现并处置潜在的安全隐患。在网络安全管理方面，还应注重风险评估和漏洞管理。定期对网络系统进行风险评估，识别潜在的安全漏洞和威胁，并制定相应的修复和加固措施^[3]。同时，建立漏洞管理机制，及时跟踪和修复已发现的漏洞，确保网络系统的安全性和稳定性。

4.3 提高用户的安全意识和操作技能

用户是网络安全防护中最薄弱的环节之一。提高用户的安全意识和操作技能对于防范网络攻击至关重要。

企业应通过定期的安全培训和教育，帮助员工了解网络安全的重要性和常见威胁类型，掌握基本的网络安全操作技能，如设置强密码、不点击可疑链接、不随意下载未知文件等。此外，建立有效的用户身份认证机制也是提升用户安全性的重要手段。通过采用多因素认证、生物识别等先进技术，可以大幅提高用户账户的安全性，防止因账户被盗用而引发的安全事件。

4.4 建立完善的网络安全应急响应机制

尽管我们可以采取各种措施来预防网络安全事件的发生，但完全避免是不可能的。因此，建立完善的网络安全应急响应机制至关重要。首先，企业应制定详细的网络安全应急预案，明确应急响应的流程、责任分工和处置措施。预案应涵盖不同类型的网络安全事件，如数据泄露、网络攻击、系统瘫痪等，确保在事件发生时能够迅速、有序地应对。其次，建立专业的应急响应团队，负责网络安全事件的监测、分析和处置工作。团队成员应具备丰富的网络安全知识和实践经验，能够迅速识别并应对各种安全威胁。同时，团队应定期进行应急演练和培训，提高应对突发事件的能力和效率。最后，加强与相关部门的合作与沟通也是建立完善的应急响应机制的重要一环。企业应积极与网络安全监管部门、公安机关等建立联系，及时获取最新的安全信息和指导，共同应对网络安全挑战。

结束语

综上所述，计算机网络安全防护是一个系统工程，需要综合运用多种技术手段和管理策略。通过不断加强安全防护措施，提高用户安全意识，建立完善的应急响应机制，我们才能有效应对日益复杂的网络安全威胁，确保计算机网络的安全稳定运行。未来，随着技术的不断进步，计算机网络安全防护将更加智能化、自动化，为数字时代的发展保驾护航。

参考文献

- [1] 龚娇, 国頔娜. 基于人工智能技术的计算机网络安全防护系统的设计和实现[J]. 软件, 2022, (04): 48-50.
- [2] 李长挺. 信息化背景下计算机网络信息安全防护策略[J]. 电子世界, 2022(13): 146-147.
- [3] 邱宜宁. 信息化时代高校计算机网络安全防护技术探究[J]. 无线互联科技, 2021, (04): 29-30.