文章类型：论文|刊号（ISSN）：2972-4112(P) / 2972-4120(O)

计算机网络安全的可靠性及优化设计问题

李肖璇
武警吉林省总队综合信息保障中心
DOI:10.12238/pe.v2i5.9898

[摘　要] 网络不仅在日常工作和商业中成为不可或缺的部分,而且在日常生活中也达到了离不开的地步。然而伴随而来的是网络安全的可靠性问题,其中增强对网络安全的可靠性研究,能够有效确保网络正常稳定运转,推动网络发展,因此本文主要研究网络安全的可靠性及其影响因素,并提出网络安全的可靠性优化设计方法,希望能够对相关从业者有所帮助。
[关键词] 计算机；网络安全；可靠性；优化设计
中图分类号：G633.67　文献标识码：A

Reliability and optimization design of computer network security

Xiaoxuan Li
Jilin Provincial Armed Police Corps Comprehensive Information Support Center
[Abstract] The network has not only become an indispensable part of daily work and business, but also reached the indispensable in daily life. However, along with the network reliability problem, which enhance the study of network reliability, can effectively ensure the normal and stable network operation, promote the development of network, so this paper mainly study network reliability and its influencing factors, and puts forward the relevant network reliability optimization design method, hope to be able to help related practitioners.
[Key words] computer; network security; reliability; optimization design

引言

现代社会中,计算机网络已成为人们日常生活和工作中不可或缺的一部分,其中网络不仅提供了便捷的信息获取途径,还可以极大地丰富了人们的娱乐和社交方式,但是如今随着网络的普及和应用,网络安全问题也日益凸显,尤其是网络可靠性问题,成为制约网络发展的关键因素之一,所以由此可见加强网络可靠性的研究和优化设计,对于保障网络安全、提升用户体验具有重要意义。

1 计算机网络安全优化设计

1.1电子邮件安全优化设计

在电子邮件安全设计中,核心在于实现数据的端到端加密(End-to-End Encryption,E2EE),这意味着邮件内容在发送端加密,仅在接收端解密,确保信息在传输过程中即便被拦截也无法被轻易解读。所以采用高级加密标准(AES)或RSA等加密算法,结合公钥基础设施(PKI)进行密钥管理,是提升邮件安全性的关键；除此以外部署邮件网关安全系统,并通过内容过滤、垃圾邮件识别、恶意软件扫描等技术,也可以有效阻挡潜在威胁,确保入站和出站邮件的纯净与安全；至于那些敏感邮件,则可引入数字签名机制,去验证邮件发送者身份及内容完整性,进一步增强信任度。

1.2网络系统的人脸识别与密码输入

为提升网络系统登录安全,融合生物识别技术如人脸识别,结合传统密码输入,构成了多因素认证(Multi-Factor Authentication,MFA)体系,其中人脸识别利用深度学习算法分析面部特征,实现高精度的身份验证,有效抵御钓鱼攻击和暴力破解；与此同时还可以引入动态令牌(OTP,One-Time Password)或手机验证码等第二因素,去进一步提升认证强度；而且加上实名制信息认证不仅限于用户名与密码,还涉及身份验证证书的绑定,确保账户与真实用户身份紧密关联,降低账户被冒用的风险,并通过持续监控异常登录行为,去及时响应并阻断潜在的安全威胁。

1.3个人信息存储与备份

在个人信息存储与备份环节,采用加密技术如AES对敏感数据进行加密存储,是保障数据安全的基础,因此可以利用云存储服务与本地存储相结合的混合云架构,去实现数据的冗余备份与灾难恢复能力,其中分布式文件系统(Distributed File System,DFS)和对象存储(Object Storage)技术可以提供高效的数据管理和扩展性,确保数据访问速度与容灾能力；除此以外实施定期的数据完整性校验(Data Integrity Check)和加密密钥轮换(Key Rotation)策略,也可以防止数据被长期窃取或篡改；最后便是利用数据脱敏(Data Masking)技术处理非必

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

要敏感信息,去减少数据泄露风险,同时满足合规性要求。

1.4系统智能访问审计

系统智能访问审计机制通过建立全面的日志收集与分析平台,实时监控网络访问行为,因此可以利用SIEM(Security Information and Event Management)工具去整合安全日志与事件信息,并结合机器学习算法去进行异常行为检测,如可以通过行为基线分析(Behavioral Profiling),为每个用户或账户建立正常行为模型,一旦发现偏离基线的访问模式,立即触发警报并采取相应安全措施；与此同时还可以引入用户与实体行为分析技术,深入挖掘潜在威胁,并利用内部威胁和高级持续性威胁智能访问审计,去提升CPU与存储资源的利用效率,从而达到减少不必要的日志存储和分析,优化系统性能,确保网络环境的持续健康与安全的目的[1]。

2 计算机网络安全的三大缺陷

2.1网络时效性

网络内容的时效性,在作为互联网特性的重要组成部分的同时,却也因此成为了钓鱼攻击(Phishing Attacks)等即时性欺诈行为的温床,特别是如今随着社交媒体、电子商务平台等实时信息流的普及,用户往往急于获取最新资讯或完成即时交易,这种紧迫性使得他们容易放松对信息来源的验证。而钓鱼者则利用这一心理去通过精心设计的假冒网站或伪装邮件,模拟合法机构的外观和流程,诱骗用户提供敏感信息如账号密码、银行账户等。这些攻击手段往往与当前热门话题、促销活动或紧急通知紧密结合,从而极大地提高欺诈成功率。

2.2网络防火墙识别不准

尽管网络防火墙作为网络安全的第一道防线,在抵御外部恶意流量方面发挥着重要作用,但其识别能力却仍存在明显局限,特别是如今随着攻击者技术的不断进步,零日漏洞(Zero-Day Vulnerabilities)的利用成为绕过防火墙的常见手段,其中零日漏洞指的是尚未被公开披露且尚未有补丁的安全漏洞,攻击者可以借此执行未授权操作或植入恶意代码；除此以外多态性攻击主要是通过动态改变恶意软件的表现形式,使得防火墙难以通过静态特征匹配进行识别。这类攻击不仅增加了检测难度,还可能导致防火墙因频繁误报而影响正常网络流量。因此,防火墙的识别能力在面对新型攻击手段时显得捉襟见肘,网络安全防护体系亟需引入更高级别的智能分析和动态防御机制。

2.3网络信息存储文件破解简易

网络信息存储文件的安全性直接关系到用户隐私和财产安全,但是由于如今许多用户因缺乏足够的安全意识,而忽视了文件加密的重要性,其会将重要数据以明文形式存储在网络中,这无疑为黑客提供了可乘之机。一旦存储系统遭受入侵或数据在传输过程中被截获,未经加密的文件将毫无防护地暴露在攻击者面前;除此以外随着计算能力的提升和破解技术的发展,即便是采用了加密算法的文件也可能面临被暴力破解的风险。因此选择强加密算法(如AES-256)并定期更换密钥已然成为保障数据安全的必要措施,与此同时实施多层防御策略,如访问控制、入侵检测和数据备份恢复,则可以进一步降低数据泄露的风险,确保网络信息存储的安全性。

3 影响计算机网络安全的主要因素

3.1网络传输设备因素

网络传输设备,如路由器(Router)、交换机(Switch)和光纤收发器(Fiber Optic Transceiver)等,作为连接不同网络节点的桥梁,其性能将会直接决定数据传输的速度与效率,而且高速传输能力还有助于减少延迟,提升用户体验;而高稳定性则能有效抵御外界干扰,防止数据丢失或损坏,因此为确保传输设备的持续高效运行,需定期进行维护检查,包括固件升级、配置优化及故障排查等,以应对可能出现的性能瓶颈和安全漏洞[2]。

3.2网络终端设备因素

网络终端设备,如个人电脑(PC)、智能手机(Smartphone)和平板电脑(Tablet)等,作为用户接入网络的主要接口,其性能与安全性同样不容忽视,且如今随着移动办公和远程访问的普及,终端设备的安全防护已然成为网络安全领域的重点之一,因此可以采用硬件级别的安全模块(HSM)、生物识别技术以及定期更新的操作系统与防病毒软件去有效抵御恶意软件的攻击,保护用户数据不被窃取或篡改,且与此同时高性能的处理器(CPU)、大容量内存(RAM)以及高速存储设备(SSD)也是提升终端设备响应速度与处理能力的关键。

4 计算机网络安全优化设计问题探究

4.1网络安全的网站优化设计

4.1.1网络钓鱼事件

现如今针对日益猖獗的网络钓鱼攻击,采用智能辨别技术(如机器学习算法、深度学习模型)对网站域名、URL链接及邮件内容进行实时分析,可以精准识别并拦截潜在的钓鱼网站,同时再结合内容安全策略(CSP)、双因素认证(2FA)以及用户教育等手段,去构建多维防护体系,也可以提升用户的防范意识与能力;除此以外还可以建立钓鱼网站黑名单数据库,去实现快速响应与阻断机制,进一步降低用户上当受骗的风险。

4.1.2捕获僵尸网络

僵尸网络(Botnet)作为网络安全的重大威胁之一,其隐蔽性强、破坏力大,因此为了有效捕获并清除僵尸网络病毒,需运用网络流量分析(NFA)、行为模式识别(BPM)以及沙箱测试等高级技术手段,去对病毒样本进行深入剖析与逆向工程,并且开发高效的病毒过滤与清除工具(如AV引擎、启发式扫描器等),实现对僵尸网络活动的实时监控与阻断；除此以外还要加强与国际安全组织及同行的合作与信息共享,共同构建全球性的僵尸网络防御体系。

4.1.3网站小插件

针对用户浏览网页时可能遭遇的恶意广告、跟踪脚本等威胁,可以开发并推广具有实时检索与拦截功能的网站小插件(Browser Extension),这些小插件体积小、安装简便,能够在不干扰用户正常浏览体验的前提下,有效过滤恶意内容、保护用户

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

隐私。同时再利用大数据分析与机器学习技术持续优化插件的识别准确性与性能表现,确保用户能够享受到更加安全、纯净的网络环境。

4.2网络层次结构优化设计

4.2.1网络模型构建

采用接入层(Access Layer)、汇聚层(Aggregation Layer)与核心层(Core Layer)相结合的三层网络模型构建策略,可以确保网络系统的稳定性与可扩展性,其中接入层负责提供用户接入与访问控制功能;汇聚层则负责将多个接入层设备的数据进行汇聚与初步处理；核心层则承担整个网络的数据交换与路由控制任务,这样通过优化各层设备间的连接方式与传输协议(如MPLS、SDN等),便可以提升网络的整体传输效率与带宽利用率。

4.2.2网络安全技术的充分应用

在网络设备与计算机设备中广泛部署防火墙、入侵检测系统(IDS/IPS)以及深度包检测(DPI)等安全设备与技术手段,可以实现对网络流量的实时监控与分析,因为其会通过运用密钥管理、加密传输(TLS/SSL)以及身份认证等技术措施保护网络安全。与此同时还可以建立全面的安全审计与日志分析机制,去对潜在的安全威胁进行快速响应与处置,或者引入人工智能(AI)与机器学习(ML)技术提升安全防御的智能化水平,实现自动化威胁识别与响应机制,构建更加智能化的网络安全防护体系。

4.2.3网络维护与设计监察

为确保网络系统的持续稳定运行需建立定期的网络维护与设计监察机制,可以通过制定详细的维护计划与实施步骤定期对网络线路、设备进行全面的检查与维护,确保设备的正常运行与性能优化,同时建立完善的网络监察体系对网络运行状态进行实时监控与分析及时发现并修复潜在故障；除此以外还可以运用网络性能管理(NPM)、网络配置管理(NCM)以及故障管理等ITIL最佳实践指导网络维护与监察工作,不断提升网络系统的整体性能与可靠性。

5 合理运用计算机网络安全的人为举措

5.1提升自身网站系统筛选

用户应主动提升对网站安全性的辨识能力,优先选择经过安全认证(如SSL证书、PCI DSS合规性认证)的网站进行访问和交易,并利用网站信誉评估工具(如Web of Trust、McAfee SECURE)去查看网站的历史安全记录和用户反馈,避免访问存在恶意软件下载、钓鱼攻击风险的未知或可疑网站；与此同时还可以关注网络安全新闻与警告,及时更新并避免访问被曝光的危险站点,从而有效防止个人信息泄露和财产损失[3]。

5.2用户通过杀毒软件的使用来维护计算机网络安全

用户应充分认识到杀毒软件在维护计算机安全中的核心作用,不仅限于安装,更要注重其日常使用与维护。选择集成云安全、行为分析、启发式扫描等高级功能的杀毒软件(如Symantec Endpoint Protection、Kaspersky Anti-Virus),去实现多层防御体系。且要做到定期执行全盘扫描,结合实时监控功能,确保及时发现并清除病毒、特洛伊木马、勒索软件等恶意程序；除此以外还要保持杀毒软件的实时更新,以应对不断演变的网络威胁,是保障计算机安全稳定运行的关键。

6 结语

总而言之,现如今随着科技的不断发展,计算机网络在人们生活和工作中的地位越来越重要,所以网络安全问题也日益凸显,所以加强网络安全的可靠性研究和优化设计是保障网络安全、提升用户体验的重要途径,因此本文通过分析计算机网络安全的可靠性问题及其影响因素,并为此提出了多种优化设计方法和人为防范措施,希望这些措施能够为提高计算机网络的安全性提供一定的参考和帮助。

[参考文献]

[1]占怡.对计算机网络可靠性优化设计问题的研究[J].通讯世界,2017,(09):148.

[2]邓伟伟.计算机网络可靠性优化设计问题分析[J].数字通信世界,2019,(04):90.

[3]张芳平.计算机网络安全的可靠性及优化设计问题探讨[J].网络安全技术与应用,2022,(06):15-17.

作者简介：

李肖璇(1984--),女,汉族,吉林长春人,硕士研究生,工程师,研究方向：计算机相关。

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.