网络通信中的数据信息安全保障技术

李 伟

江苏自动化研究所 江苏 连云港 222006

摘要：网络通信中的数据信息安全保障技术是现代信息技术领域的核心议题。本文综述了数据加密、防火墙与入侵检测系统、身份认证与访问控制等关键技术，以及安全管理制度、安全架构与系统设计、应急响应与灾难恢复计划等保障策略。这些技术和策略共同构成了网络通信中数据安全的多层次防护体系，旨在有效应对各种安全威胁，确保数据的机密性、完整性和可用性。本文的研究对于提升网络通信中的数据信息安全水平具有重要意义。

关键词：网络通信；数据信息安全；保障技术

1 网络通信中的数据信息安全概述

在网络通信日益频繁的今天，数据信息安全成为了至关重要的议题。数据信息安全主要涉及数据的保密性、完整性和可用性。保密性确保信息在传输过程中不被未授权者获取，完整性则保证数据在传输和存储过程中不被篡改或破坏。同时，可用性确保授权用户能够随时访问所需信息。为实现数据信息安全，需要采取多种技术手段，如加密技术、防火墙、入侵检测系统等。这些技术共同构建起一道坚固的安全防线，有效抵御外部攻击和内部泄露风险。数据信息安全并非一成不变，随着技术的不断进步和威胁的不断演变，我们需要不断更新安全策略和技术手段，以应对新的挑战。只有保持高度警惕和持续投入，才能确保网络通信中的数据信息安全，维护个人、企业和我国的利益。

2 网络通信中的数据信息安全威胁分析

2.1 黑客攻击与病毒传播

在网络通信中，黑客攻击是数据信息安全面临的主要威胁之一。黑客利用漏洞、恶意软件等手段，试图非法侵入系统，窃取、篡改或破坏数据。病毒传播也是一大隐患，病毒通过邮件、文件传输等途径迅速扩散，一旦感染，可能导致系统瘫痪、数据丢失等严重后果。这些攻击不仅威胁到数据的保密性和完整性，还严重影响系统的正常运行。

2.2 数据泄露与窃取

数据泄露与窃取是网络通信中另一大安全威胁。由于系统漏洞、管理不善或员工疏忽等原因，敏感数据可能被泄露给未经授权的第三方，或被恶意窃取^[1]。这些数据可能包括个人隐私、商业秘密等，一旦泄露，将对个人和企业造成巨大损失。

2.3 网络钓鱼与欺诈

网络钓鱼与欺诈是网络通信中常见的安全威胁。攻

击者通过伪装成合法机构或个人，发送虚假信息或链接，诱骗用户点击或提供个人信息。一旦用户上钩，攻击者就能获取用户的敏感信息，进而进行欺诈活动。这种威胁不仅损害用户的经济利益，还破坏网络环境的信任基础。

2.4 身份冒用与非法访问

身份冒用与非法访问是网络通信中的又一重要威胁。攻击者通过窃取或伪造用户身份，试图非法访问系统或数据。这种威胁不仅破坏了数据的保密性和完整性，还可能导致系统被恶意控制，进而引发更严重的安全问题。

3 网络通信中的数据信息安全保障技术

3.1 加密技术

加密技术是网络通信中数据安全的核心保障之一。它通过特定的算法，将明文数据转换为难以解读的密文数据，确保数据在传输过程中不被未经授权的人员获取或篡改。加密技术主要分为对称加密和非对称加密两种类型。对称加密采用相同的密钥对数据进行加密和解密。这种加密方式具有速度快、效率高的优点，适用于大量数据的加密处理。然而对称加密的密钥分发和管理是一个挑战，因为发送方和接收方需要事先约定好密钥，并在通信过程中保密。常见的对称加密算法包括DES、3DES和AES等。这些算法通过复杂的数学运算，将明文数据转换为看似随机的密文数据，从而保护数据的机密性。非对称加密则使用一对密钥，即公钥和私钥，进行加密和解密操作。公钥用于加密数据，私钥用于解密数据。由于公钥可以公开，而私钥必须保密，因此非对称加密在密钥分发方面具有更高的安全性。非对称加密的加密和解密速度相对较慢，适用于对少量数据进行加密处理。常见的非对称加密算法有RSA、ECC等。这些算法通过复杂的数学运算，确保只有持有私钥的一

方才能解密数据,从而保护数据的机密性和完整性。加密技术的应用不仅限于数据传输过程中,还可以用于存储数据的保护。全磁盘加密技术也可以对整个磁盘进行加密,确保即使磁盘被非法获取,数据也无法被轻易读取。

3.2 防火墙与入侵检测系统

防火墙和入侵检测系统是网络通信中数据安全的重要防线。防火墙位于内部网络与外部网络之间,通过预定义的安全规则过滤进出的数据包,阻止潜在的威胁进入网络。防火墙的工作原理基于包过滤技术,它会检查每个数据包的头部信息,包括源地址、目的地址、端口号等,并根据这些信息与预先设定的安全策略进行比较^[2]。只有符合规则的数据包才会被放行,从而确保网络的安全。防火墙的类型多种多样,包括包过滤防火墙、应用级网关防火墙、状态检测防火墙和下一代防火墙等。包过滤防火墙是最基础的类型,只检查数据包头部信息。应用级网关防火墙则能够理解特定的应用层协议,并进行更深入的内容检查。状态检测防火墙结合了包过滤和应用级网关的优点,能够跟踪连接的状态,提供更高效且安全的服务。下一代防火墙则除了传统的防火墙功能外,还集成了高级功能如应用识别、用户身份验证、入侵防御等。入侵检测系统(IDS)是另一种重要的安全工具,它能够监控网络或系统的活动,寻找可疑行为或安全政策违规迹象。一旦发现潜在威胁,IDS会生成警报,并可能采取行动阻止入侵。IDS通过分析网络流量或主机系统的活动来检测异常行为,可以基于已知的攻击模式(签名)或通过行为分析来识别潜在的威胁。基于网络的IDS(NIDS)部署在网络的关键位置,监控整个网络的流量;而基于主机的IDS(HIDS)则安装在单个主机上,监控该主机上的文件和活动。防火墙和IDS通常协同工作,以提供更全面的保护,防火墙作为第一道防线,通过过滤机制阻止非法访问;而IDS则通过监测网络活动,帮助组织及时发现并响应潜在的安全威胁。这种组合使得网络通信中的数据信息安全得到了更有效的保障。

3.3 身份认证与访问控制技术

身份认证与访问控制技术是网络通信中数据安全的关键环节。身份认证技术通过验证用户的身份信息,确认其是否具有访问权限。常见的身份认证方式包括密码认证、生物特征认证和数字证书认证等。密码认证是最常见的身份认证方式之一,用户通过输入正确的用户名和密码来验证身份。密码认证存在一些问题,如用户容易设置简单密码、密码泄露的风险较高等。结合其他验证方式如生物特征认证或数字证书认证来提高安全性是必要的。生物特征认证通过识别用户的生物特征来进

行身份验证,如指纹识别、面部识别、虹膜识别等。这种技术相比于密码认证更为安全,因为生物特征是每个人独有的,难以伪造。生物特征认证技术也存在一些问题,如识别准确率不高、设备成本较高等。数字证书认证则是基于公钥加密技术的身份认证方式,通过证书机构颁发的数字证书来验证用户身份和数据的完整性。数字证书认证在互联网通信、电子商务等领域得到广泛应用,其安全性和可信度较高。访问控制技术则通过权限管理和身份认证等手段,对网络通信中的数据进行控制和保护。常见的访问控制技术包括访问控制列表(ACL)和防火墙等。ACL是一种基于规则的访问控制技术,用于管理网络资源的访问权限。ACL定义了不同用户对资源的访问规则和权限,可以通过配置ACL来限制特定用户的访问权限。防火墙则通过检查和过滤进出网络的数据包,防止恶意访问和攻击。身份认证与访问控制技术的应用不仅限于网络登录和系统资源访问控制,还可以用于数据加密、远程访问控制等方面。通过加强身份认证和访问控制技术的应用,可以有效地防止未经授权的用户访问系统和网络资源,保护用户信息的安全。

3.4 数据备份与恢复技术

数据备份是指将重要数据复制到另一个存储介质或位置,以防止原始数据因各种原因(如硬件故障、病毒攻击、人为错误等)而丢失。通过定期备份数据,可以确保在数据丢失或损坏时,能够迅速恢复到最近一次备份的状态,从而最大限度地减少损失。数据备份策略通常包括全备份、增量备份和差异备份,全备份是指复制所有选定文件和文件夹,适用于首次备份或重要数据更新后^[3]。增量备份则只备份自上次备份以来发生变化的文件,可以大大减少备份所需的时间和存储空间。差异备份则备份自上次全备份以来发生变化的所有文件,结合了全备份和增量备份的优点,既保证了数据的完整性,又提高了备份效率。数据恢复技术是在数据丢失或损坏后,利用备份数据进行恢复的过程。恢复操作通常包括识别丢失或损坏的数据、定位备份数据、恢复数据以及验证数据完整性等步骤。

3.5 虚拟专用网络(VPN)技术

虚拟专用网络(VPN)技术是一种通过公共网络建立加密通道,实现远程用户或分支机构与总部之间安全通信的技术。VPN技术通过封装和加密数据,确保数据在传输过程中不被未经授权的人员窃取或篡改,同时保证数据传输的完整性和机密性。VPN技术主要分为SSL VPN和IPSec VPN两种类型,SSL VPN基于Web浏览器,

用户无需安装额外的客户端软件,只需通过浏览器访问VPN网关,输入用户名和密码即可建立安全连接。这种技术适用于远程办公、移动办公等场景,具有易于部署和使用的优点。IPSec VPN则是一种端到端的加密协议,通过在网络层对数据进行加密和认证,确保数据在传输过程中的安全性。VPN技术的应用不仅限于数据加密和认证,还可以实现访问控制、网络隔离等功能。通过配置VPN策略,可以限制特定用户或设备的访问权限,防止未经授权的访问和数据泄露。VPN技术还可以将不同地理位置的网络资源连接成一个虚拟的专用网络,实现资源共享和协同工作,提高业务效率和安全性。

4 网络通信中的数据信息安全保障策略

4.1 安全管理制度与规范建设

网络通信中的数据信息安全保障,首要在于建立健全的安全管理制度与规范。这些制度与规范是确保数据安全的基础,它们为组织内部的数据处理、存储、传输和访问提供了明确的指导和约束。安全管理制度应涵盖数据分类、权限管理、访问控制、加密解密、审计监控等多个方面,确保数据的全生命周期都得到有效的保护。在制度建设上,企业应明确数据安全的责任主体,制定详细的数据安全管理流程,包括数据的收集、存储、使用、共享和销毁等环节。应建立数据泄露的应急预案,确保在数据泄露事件发生时能够迅速响应,减少损失。企业还应定期对员工进行数据安全培训,提高员工的安全意识和操作技能,确保制度的有效执行。规范建设方面,企业应遵循国家法律法规和行业标准,制定符合自身业务特点的数据安全规范。这些规范应明确数据的安全等级、保护措施、访问权限、审计要求等内容,确保数据在各个环节都得到合规处理。

4.2 安全架构与系统设计

安全架构与系统设计是网络通信中数据安全保障的核心。在设计安全架构时,企业应充分考虑数据的敏感性、业务需求和安全威胁,采用分层防御、最小权限原则、访问控制等策略,构建多层次的安全防护体系。在系统设计上,企业应采用安全的技术架构和组件,如使用加密技术保护数据传输和存储,采用防火墙、入侵检测系统等技术手段防范外部攻击。企业应注重系统的可

用性和冗余性设计,确保在单点故障发生时,系统能够迅速恢复并继续提供服务。企业还应定期对系统进行安全评估和漏洞扫描,及时发现并修复潜在的安全漏洞^[4]。在系统设计过程中,企业应充分考虑用户隐私和数据保护的需求,遵循最小数据收集原则,避免过度收集用户信息。企业应建立数据访问和使用的审批机制,确保数据的合法使用和共享。

4.3 应急响应与灾难恢复计划

应急响应与灾难恢复计划是网络通信中数据安全保障的重要组成部分。面对可能发生的数据泄露、网络攻击等安全事件,企业需要制定详细的应急响应计划,确保在事件发生时能够迅速响应、有效处置。应急响应计划应包括事件报告流程、应急处置流程、数据恢复流程等内容,确保在事件发生时能够迅速定位问题、隔离风险、恢复业务。在灾难恢复计划方面,企业应建立数据备份和恢复机制,确保在数据丢失或损坏时能够迅速恢复数据。企业应定期进行灾难恢复演练,验证备份数据的可用性和恢复流程的有效性。通过不断完善应急响应和灾难恢复计划,企业可以提高应对安全事件的能力和效率,确保网络通信中的数据信息安全。

结束语

网络通信中的数据信息安全保障是一个复杂而系统的工程。通过综合运用多种技术和策略,可以构建更加安全可靠的网络通信环境。随着技术的不断进步和安全威胁的不断演变,也需要不断更新和完善保障措施。未来,将继续探索更加高效、智能的数据安全保障技术,为网络通信中的数据信息安全提供更加坚实的保障。

参考文献

- [1]康海连.网络通信中的数据信息安全保障技术[J].信息记录材料,2021,22(09):71-72.
- [2]官月月,郭建勤,张胜平.网络通信中的数据信息安全保障技术研究[J].无线互联科技,2021,18(16):3-4.
- [3]杨志贞.网络通信中的数据信息安全保障技术研究[J].电子测试,2021,(11):137-138.
- [4]孟祥智.网络通信中的数据信息安全保障技术[J].通讯世界,2020,27(7):109-110.