局域网环境下的计算机网络安全技术研究

宫敬原，刘 萍
（郑州工业应用技术学院 河南 郑州 451100）

【摘要】随着信息技术的迅猛发展，局域网在企业、学校、政府机构等领域得到广泛应用，大大提升了信息共享效率与团队协作水平，但局域网环境下的计算机网络安全问题不容小觑。因此，本文将围绕局域网环境下的计算机网络安全技术展开研究，首先，概述局域网与计算机网络安全的基本概念，强调保证网络安全的重要性。其次，从技术角度出发深入分析局域网环境下计算机网络安全面临的主要问题，针对问题详细探讨多种网络安全技术的应用策略，包括使用杀毒软件、应用防火墙技术、采用加密技术、加强授权管理以及采用虚拟局域网技术等，旨在为局域网的安全管理提供理论支持和实践指导。

【关键词】局域网；计算机；网络安全；加密
【中图分类号】TP309.2 【文献标识码】A 【文章编号】1009-5624(2024)12-0125-03

0 引言

随着信息技术的飞速发展，计算机网络已成为现代社会不可或缺的基础设施，而局域网（local area network，LAN）作为网络的重要组成部分，在企业、学校、政府机构等各个领域中得到了广泛应用，在提高信息共享效率、促进团队协作等方面发挥着重要作用。然而，随着网络技术的不断进步和网络应用的日益复杂，局域网环境下的计算机网络安全问题也日益凸显，数据泄露、病毒攻击、黑客入侵等威胁层出不穷，这些事件不仅导致敏感信息的泄露，还造成重大的经济损失和声誉损害。因此，对局域网环境下的计算机网络安全技术进行深入研究，提升网络安全防护能力，显得极为关键，也是眼下亟待解决的重要课题。

1 局域网与计算机网络安全概述

1.1 LAN

LAN 是一种在小范围内（如学校、企业、机关等）实现计算机设备、服务器、打印机及其他网络设备互联互通的网络系统，主要通过高速通信线路（如同轴电缆、双绞线、光纤等）或无线电波，将各种设备连接在一起，形成资源共享和数据传输的网络环境[1]。局域网的主要特点是传输速度快、延迟小、误码率低，一般归属于单一组织，便于管理和控制。在局域网中，数据可以在各个设备之间高效传输，用户能够轻松访问共享资源，如文件、打印机等，从而能显著提高工作效率和便利性。

1.2 计算机网络安全

计算机网络安全则是指保护计算机网络系统中的硬件、软件及其系统中的数据不受偶然或恶意的原因而遭到破坏、更改或泄露，确保系统能连续、可靠、正常地运行，同时保障网络服务不中断，主要涉及网络系统的各个方面，包括数据的机密性、完整性、可用性、可控性和可审查性等。在计算机网络日益成为人们生活、工作重要组成部分的今天，网络安全问题显得尤为重要，计算机网络安全不仅包括防止外部攻击和入侵，还包括防范内部泄露和滥用。为了实现网络安全，需要综合运用加密技术、防火墙、入侵检测系统、用户身份认证等各种技术手段和管理措施，构建多层次、全方位的安全防护体系[2]。当然，网络安全也是一个持续的过程，需要不断更新和改进安全措施，以应对不断变化的网络威胁。

2 局域网环境下保证计算机网络安全的重要性

从信息保密性的角度来看，局域网作为企业、机构内部信息共享与交流的重要平台，承载着大量的敏感数据和关键信息，比如商业机密、客户资料、研发成果等，一旦信息泄露不仅会导致知识产权的损失，还可能对组织的竞争力产生严重影响，甚至引发法律纠纷。因此，确保局域网环境下计算机网络的安全，是保护组织核心信息资产、维护商业利益不受侵犯的关键所在。

从系统稳定性的角度考虑，局域网中的计算机网络安全直接关系到整个网络的可靠运行。局域网中的设备相互连接，共享资源，若其中一台设备受到安全威胁，如病毒攻击或恶意软件的入侵，这种威胁会迅速蔓延至整个网络，导致网络服务中断、数据损坏或丢失，进而影响正常的工作流程和业务运作[3]。此外，随着物联网、云计算等新技术在局域网环境中的应用，网络安全问题变得更加复杂多样，保证计算机网络安全不仅能够防范外部攻击，还能确保内部系统的稳定性和业务的连续性，为组织提供安全、高效的网络环境。

3 局域网环境下计算机网络安全面临的问题

局域网环境下的计算机网络安全问题是一个多层次、多维度的复杂系统问题，下文将从技术角度出发深入分析局域网所面临的主要安全问题，这些问题的存在严重威胁着局域网的安全性，可能导致敏感信息的泄露、系统损坏，甚至整个网络的瘫痪。

3.1 数据泄露

由于局域网内部的数据传输频率高且数据量大，如果没有得到充分的加密和保护，敏感数据很容易被非法访问和窃取。数据泄露通常发生在数据传输、存储或处理的过程中，可能由网络监听、恶意软件感染，或者系统漏洞等原因导致。从技术的角度来看，数据泄露的根源在于网络通

作者简介：宫敬原（2004—），男，河南洛阳，本科，研究方向：计算机网络安全。

信和数据存储的安全性不足，假如局域网中使用的是明文传输协议，那么攻击者就可以通过网络监听工具轻易地截获传输中的数据；如果数据库或文件系统的访问控制不严格，也可能导致未授权用户访问敏感数据[4]。数据泄露的危害是巨大的，不仅会导致个人隐私泄露，还可能使企业或机构的商业机密被曝光，从而造成重大的经济损失或承担严重的法律责任，因此防止数据泄露是局域网安全的首要任务之一。

3.2 病毒攻击

病毒是一种恶意软件，能够复制自身并在网络中传播，从而破坏数据、干扰计算机操作，甚至导致系统崩溃，在局域网环境中病毒的传播速度更快，影响范围更广。一般来讲，病毒主要通过电子邮件附件、恶意网站下载、移动存储设备等方式传播，一旦局域网中的某台计算机被病毒感染，病毒就会利用局域网中的共享资源和网络通信机制迅速扩散到其他计算机，而且这一扩散过程往往是隐蔽且迅速的，很难被及时发现和控制。遭受病毒攻击后，数据和文件系统会被破坏，还可能导致网络拥堵、系统崩溃等问题，更为严重的是一些高级病毒还具有窃取信息、进行勒索等恶意功能，给用户带来巨大的经济损失和隐私泄露风险。

3.3 黑客攻击

黑客利用各种技术手段非法侵入他人的计算机系统，窃取、篡改或破坏数据，甚至控制整个网络。在局域网环境中，黑客攻击的形式多样，比如网络钓鱼、恶意代码注入、拒绝服务攻击（denial-of-service attack，，DOS）等。无论黑客攻击的技术手段如何翻新，其核心原理都是利用系统或应用的漏洞进行入侵，比如利用局域网中某些设备的默认密码或弱密码进行暴力破解，从而获得设备的控制权；通过伪造 IP 数据包、利用传输控制协议/网际协议（transmission control protocol/internet protocol，TCP/IP）中的漏洞等方式进行网络攻击。黑客攻击不仅会导致数据泄露和损坏，还可能使整个网络陷入瘫痪状态，并且还可能利用被控制的计算机进行进一步的攻击活动，比如发起分布式拒绝服务攻击等，给整个网络带来更大的安全隐患[5]。

3.4 漏洞利用

漏洞是指计算机系统或应用中存在的安全缺陷，可能被攻击者利用来执行未授权的操作或访问敏感数据。由于局域网环境中存在多样的设备和应用，所以漏洞的存在不可避免。漏洞利用的形式多种多样，比如缓冲区溢出、结构化查询语言注入、跨站脚本攻击等，具体攻击方式均利用了系统或应用中的安全漏洞来执行恶意代码或获取敏感信息。举例来讲，缓冲区溢出攻击就是通过向系统输入超出其缓冲区大小的数据来覆盖相邻的内存区域，从而执行攻击者植入的恶意代码。漏洞利用的危害巨大，不仅会导致数据泄露和系统损坏，还可能使整个网络陷入安全风险之中，一些高级漏洞利用技术还可以绕过安全防御系统，直接攻击网络的核心部分，给整个局域网带来毁灭性的打击。

4 局域网环境下计算机网络安全技术的应用

4.1 使用杀毒软件

在局域网环境下，杀毒软件能够检测、隔离和清除病毒、木马、蠕虫等恶意软件，从而有效防止这些恶意软件在网络中传播和造成损害。因此，网络管理员需要选择一款信誉良好、更新及时、检测率高的杀毒软件，重点考虑软件的病毒库更新频率、系统资源占用情况以及是否支持实时监控等因素。首先，对局域网中的所有计算机进行杀毒软件的统一安装，可以利用局域网的管理工具进行远程推送和安装，确保每一台计算机都受到保护，同时设置为自动更新病毒库，以便及时应对新出现的病毒威胁[6]。其次，启用杀毒软件的实时监控功能，对系统的关键区域进行持续监控，一旦发现可疑文件或行为，立即进行隔离和处理，并且要切记定期进行全面系统扫描，力求发现并清除可能潜伏的恶意软件。最后，还可以利用杀毒软件的网络防护功能，对进出局域网的数据流进行监控和过滤，阻止恶意代码的传入和敏感信息的泄露。为了进一步提高安全性，可以利用路由器的功能来屏蔽所有不必要的 IP 地址，只允许办公所需的 IP 地址访问网络，有效减少潜在攻击面，降低被攻击的风险。

4.2 应用防火墙技术

防火墙技术能够有效地拦截和监视网络中的数据包，保护局域网络不受未经授权的访问。在局域网环境下，防火墙应部署在局域网的入口处，即连接局域网和外部网络的边界处，以便对所有进出局域网的数据流进行监控和过滤。防火墙规则的设置应基于“最小权限原则”，即只允许必要的网络通信通过，严格限制不必要的网络访问，具体做法应定义允许或拒绝的数据包类型、来源和目的地 IP 地址、端口号以及通信协议等。比如，可以设置规则以允许内部网络的超文本传输协议和超文本传输安全协议流量通过，同时阻止所有来自未知 IP 地址的因特网控制报文协议请求，从而减少网络攻击的风险[7]。需要定期更新防火墙的规则库和签名数据库，原因在于网络安全威胁不断变化，新的攻击手法和漏洞利用方式层出不穷，通过定期更新可以确保防火墙能够识别并防御最新的安全威胁。此外，防火墙应能够记录所有通过其的数据流，并提供报告和警报功能，日志可以用于分析网络流量模式，检测异常行为，并在发生安全事件时进行取证。当然，为了确保防火墙的有效性，应定期进行安全评估和渗透测试，模拟真实的网络攻击，检验防火墙的防御能力，并发现可能存在的安全漏洞。

4.3 采用加密技术

加密技术通过对数据进行变换，使得未经授权的用户无法读取或理解数据的原始内容，从而保护数据的机

密性和完整性。针对数据传输过程中的加密，推荐使用安全套接层（secure socket layer，SSL）或安全传输层协议（transport layer security，TLS），能够在客户端和服务器之间建立安全的加密连接，确保数据在传输过程中不被窃取或篡改[8]。实施时，应在服务器端配置 SSL/TLS 证书，验证服务器的身份，并在客户端和服务器之间建立安全的加密通道；针对存储在局域网中的敏感数据，可以采用高级加密标准（advanced encryption standard，AES）或一种非对称加密算法（rivest-shamir-adleman，RSA）等进行加密。AES 算法适用于大量数据的加密，其密钥长度可选，提供不同级别的安全性，因此需选择合适的密钥长度，并确保密钥的安全存储和管理。而 RSA 则适用于数字签名和密钥交换等场景，解决了大数分解问题的困难性。

为了进一步提高加密的灵活性和安全性，可以采用混合加密方案，使用对称加密算法（如 AES）加密实际数据，而使用非对称加密算法（如 RSA）加密对称加密算法的密钥，既能保证加密的高效性，又能确保密钥分发的安全性。在实施加密技术时，还需注意以下方面：①确保加密算法和密钥的安全性，避免使用已被破解或存在已知漏洞的加密算法；②要定期更换密钥，减少密钥被破解的风险；③建立完善的密钥管理制度，包括密钥的生成、分发、存储、使用和销毁等环节。

4.4 加强授权管理

完善授权管理可以精细控制用户对网络资源的访问权限，从而有效防止未授权访问和数据泄露。在局域网环境下，应实施基于角色的访问控制（role-based access control，RBAC）策略，根据用户的角色和职责来分配权限，确保每个用户只能访问其工作所需的最小资源集。例如，可以为网络管理员、普通员工、访客等不同角色设置不同的访问权限。在实施 RBAC 时，应利用局域网内的身份验证系统，如轻型目录访问协议或 Active Directory，来集中管理用户身份和权限信息。除了传统的用户名和密码验证外，应采用多因素身份验证方法，如引入生物识别技术（如指纹识别、面部识别）或动态令牌等作为第二重身份验证手段，降低账户被非法接管的风险。

在实施授权管理的过程中，需要注意日志记录和监控，所有用户的访问时间、访问的资源、执行的操作等访问行为都应被详细记录，用于事后审计和追踪安全事件。同时，应利用安全信息和事件管理系统对日志进行实时监控和分析，及时发现并响应异常访问行为。为了提高授权管理的效率和准确性，可以使用身份和访问管理软件来自动化用户账户的创建、修改和删除过程，减少人为错误和延迟。

4.5 采用虚拟局域网技术

在局域网环境中，采用虚拟局域网（virtual local area network，VLAN）技术能够将物理上处于同一局域网内的不同用户从逻辑上划分成不同的广播域，进而有效地隔离广播风暴，提高网络性能，同时也能增强网络的安全性。实施 VLAN 技术，首先需要对网络设备进行配置，一般需要对网络交换机进行合理配置，根据特定的规则来划分不同的 VLAN，可以基于端口、媒体存取控制地址（media access control address，MAC）、IP 地址或协议等因素。

在实施 VLAN 划分时，应遵循以下步骤：①规划 VLAN 结构。明确网络中需要划分的 VLAN 数量、名称以及每个 VLAN 所包含的端口或设备。②配置 VLAN。在网络交换机上创建相应的 VLAN，并为其分配唯一的 VLAN ID，同时设置 VLAN 的名称以便于管理。③分配端口。将交换机的端口分配到相应的 VLAN 中，通过静态配置或基于 MAC 地址、IP 地址的动态配置来实现。④配置 VLAN 间路由。不同 VLAN 之间需要通信，则需要配置 VLAN 间路由，一般通过在交换机上启用三层路由功能或使用专门的路由器来实现。⑤验证配置。在完成 VLAN 配置后，应进行详细的测试以验证配置的正确性，比如检查 VLAN 间的隔离性、通信的可达性以及网络性能等。⑥持续监控与维护。定期对 VLAN 配置进行审查和更新，适应网络环境和业务需求的变化，建立有效的监控机制及时发现并解决潜在的网络安全问题。

5 结语

综上所述，局域网环境下的计算机网络安全是一个复杂而重要的课题，面对不断变化的网络威胁和挑战，相关研究者必须持续关注和研究新的安全技术和方法，确保网络的安全性和稳定性。本文提出的多种网络安全技术应用策略，旨在从多个层面构建全面、有效的安全防护体系，为局域网的安全管理提供有力的技术支持。然而，网络安全是永无止境的过程，需要不断更新和改进安全措施，才能适应日益复杂的网络环境和安全需求。

【参考文献】

[1] 韩阳，石颖. 局域网环境下计算机网络安全防护技术应用研究 [J]. 中国新通信，2022，24(16)：113-115.
[2] 彭怀龙，褚含冰. 局域网环境下的计算机网络安全技术应用分析 [J]. 数字技术与应用，2023，41(4)：228-230.
[3] 陈辉江. 校园局域网环境下计算机网络安全与防范措施初步探讨 [J]. 办公自动化，2022，27(13)：49-51，23.
[4] 刘煜. 利用数据处理技术开展计算机网络安全存储系统设计 [J]. 科技与创新，2024(8)：89-91，94.
[5] 白天毅. 局域网环境背景下的计算机网络安全技术应用探析 [J]. 网络安全技术与应用，2023(8)：19-21.
[6] 耿亚涛. 计算机网络技术在电子信息工程应用中的研究 [J]. 科技经济市场，2023(10)：29-31.
[7] 柯秀清. 计算机网络安全技术在网络安全维护中的应用 [J]. 中国新通信，2023，25(20)：65-67.
[8] 覃卫华. 计算机网络安全中的虚拟网络技术研究 [J]. 信息与电脑(理论版)，2023，35(20)：183-186.