计算机网络与信息安全系统的建立与技术探究

宁召宇
1. 中国民用航空飞行学院洛阳北郊机场　河南　洛阳　471000
2. 洛阳北郊机场有限责任公司　河南　洛阳　471000

摘　要：计算机网络与信息安全系统的构建至关重要。本文先分析网络面临的安全威胁，包括共享开放特性带来的风险、病毒恶意软件攻击、网络入侵及用户操作管理漏洞等。接着从物理环境、运行环境、软件及数据环境三方面阐述系统构建措施，如物理安全防护、制度管理、设备备份、信息传输防护、系统完善、权限划分等。最后探究关键技术，像防火墙、入侵检测、加密和访问控制技术，为计算机网络与信息安全系统的建立与技术应用提供参考。

关键词：计算机网络；信息安全系统；建立；技术

引言：在数字化时代，计算机网络已深度融入社会各领域，信息传输与处理效率大幅提升，但安全问题也日益严峻。网络的共享性与开放性在带来便利的同时，使系统面临病毒、恶意软件、网络攻击等多重威胁，用户操作不当和管理漏洞更是加剧了安全风险。构建可靠的计算机网络与信息安全系统，探究有效的安全技术，成为保障网络稳定运行、保护信息安全的迫切需求。本文将分析安全威胁，探讨系统构建及关键技术，为信息安全保障提供思路。

1 计算机网络面临的安全威胁分析

1.1 网络的共享性与开放性威胁

计算机网络的共享性与开放性是其核心优势，却也成为安全隐患的温床。在共享环境下，用户可便捷获取与传输信息，但网络边界的模糊化使得非法用户能轻易渗透，未经授权访问系统资源。开放性使得网络协议和服务暴露在公共环境中，攻击者可利用协议漏洞发起攻击，如 TCP/IP 协议的缺陷易导致拒绝服务攻击 。同时，网络节点间频繁的数据交互，增加了数据被窃取、篡改的可能性，信息在开放的传输过程中面临着被监听、泄露的风险，严重威胁用户隐私与数据安全。

1.2 病毒与恶意软件攻击

病毒与恶意软件是计算机网络的主要威胁之一。病毒可通过网络快速传播，感染大量计算机设备，破坏系统数据、干扰正常运行。恶意软件类型多样，如木马病毒会伪装成正常程序，潜伏在用户设备中，窃取账号密码、个人隐私等敏感信息；勒索软件则对数据进行加密，向用户索要赎金以解锁文件。随着技术发展，恶意软件传播途径不断拓展，除传统的邮件、移动存储设备，还通过恶意网站、免费软件捆绑等方式入侵，且部分恶意软件具备自我变异能力，躲避安全防护软件的查杀，加大了防范难度。

1.3 网络攻击与入侵

网络攻击与入侵手段层出不穷，严重威胁网络安全。黑客常采用暴力破解、SQL 注入等技术手段，获取系统权限，窃取敏感数据。分布式拒绝服务（DDoS）攻击通过控制大量 “僵尸” 主机，向目标服务器发送海量请求，使其资源耗尽无法正常服务。此外，中间人攻击会拦截、篡改通信双方的数据，破坏数据完整性与机密性。新型攻击如物联网设备漏洞利用攻击，利用智能设备安全防护薄弱的特点，将其纳入攻击网络，扩大攻击规模与影响范围，给网络安全带来新的挑战。

1.4 用户操作不当与管理漏洞

用户操作不当与管理漏洞为网络安全埋下隐患。用户安全意识不足，设置简单密码、随意连接公共 Wi-Fi、下载不明来源文件，易导致账号被盗、设备感染病毒。部分用户未及时更新系统补丁，使设备暴露在已知漏洞风险下。在管理层面，网络安全管理制度不完善，缺乏严格的权限管理与审计机制，无法有效约束用户行为，出现越权操作、权限滥用等问题。同时，网络安全应急响应机制不健全，在安全事件发生时，导致损失扩大[1]。

2 计算机网络与信息安全系统的构建

2.1 系统物理环境安全措施

系统物理环境安全是信息安全的基础防线。首先，机房选址需远离自然灾害高发区、强电磁干扰源等，确保物理环境稳定。机房应配备门禁系统，严格限制人员进出，通过指纹、刷卡、密码多重验证方式，防止无关人员进入。同时，安装监控设备，24 小时实时监控机房动态，及时发现异常情况。此外，针对供电系统，配备不间断电源（UPS）和柴油发电机，保障电力持续供应；设置防火、防水、防潮、防静电设施，避免因火灾、渗

水、静电等物理因素对设备和数据造成损坏，全方位保障系统物理环境安全。

2.2 系统运行环境安全措施

2.2.1 加强制度管理

完善的制度管理是保障系统运行环境安全的重要支撑。制定严格的人员管理制度，明确各岗位人员的职责与权限，禁止越权操作，对涉及敏感信息处理的人员进行背景审查与定期考核。建立网络安全操作规范，要求用户使用强密码并定期更换，规范软件下载、数据传输等操作流程，避免因人为失误引发安全问题。同时，设立安全审计制度，对系统操作、数据访问等行为进行实时记录与审计，及时发现违规操作与安全隐患。此外，还需建立安全培训机制，定期对员工开展网络安全知识培训，提升全员安全意识与应急处理能力。

2.2.2 设备备份与冗余设计

设备备份与冗余设计可有效提升系统的可靠性与容错能力。对关键网络设备、服务器等进行定期备份，包括硬件配置信息、系统软件、应用软件及数据等，确保在设备故障或数据丢失时能够快速恢复。采用冗余设计方案，如服务器双机热备，当主服务器出现故障时，备用服务器可立即接管服务，保障业务连续性。在网络架构方面，构建冗余网络链路，避免因单一链路故障导致网络中断。通过存储设备的冗余配置，如磁盘阵列（RAID）技术，防止因磁盘损坏造成数据丢失，从多方面保障系统设备安全稳定运行。

2.2.3 信息传输通道安全防护

信息传输通道安全防护是防止数据泄露与篡改的关键环节。对传输数据进行加密处理，采用先进的加密算法，如 AES、RSA 等，确保数据在传输过程中即使被窃取也无法被轻易破解。在网络边界部署防火墙，对进出网络的数据进行过滤与监测，阻止非法访问与恶意攻击。同时，使用虚拟专用网络（VPN）技术，在公用网络上建立专用加密通道，保障远程数据传输安全。此外，定期对传输通道进行安全检测与维护，及时修复发现的漏洞，防止攻击者利用通道缺陷进行数据拦截、篡改等操作，保障信息传输的安全性与完整性。

2.3 系统的软件及数据环境安全措施

2.3.1 及时完善操作系统

操作系统是计算机运行的基础，其安全性直接影响整个系统。随着网络技术发展，各类漏洞不断被发现，若不及时修复，易成为黑客攻击的突破口。因此，需建立完善的操作系统更新机制，及时获取并安装官方发布的补丁程序，封堵安全漏洞，抵御诸如缓冲区溢出、代码执行等类型的攻击。同时，对操作系统的服务与功能进行合理配置，关闭不必要的服务端口，减少系统暴露面。定期对操作系统进行安全扫描与评估，检测潜在的安全隐患，确保操作系统始终处于安全、稳定的运行状态，为上层应用和数据提供可靠的运行环境。

2.3.2 划分用户权限

科学划分用户权限是保障数据安全、防止越权操作的有效手段。根据用户的工作职责与需求，严格界定其对系统资源和数据的访问、操作权限。对于普通用户，仅赋予完成日常工作所需的最小权限，如只读某些文件或执行特定程序；而管理员权限则需严格管控，仅授予少数可信人员，并对其操作进行严格审计。通过权限分级管理，可避免因用户误操作或恶意行为导致的数据泄露、篡改等问题。同时，定期对用户权限进行审查与调整，确保权限分配与实际工作需求相匹配，随着人员岗位变动及时更新权限设置，最大限度降低权限管理带来的安全风险。

2.3.3 物理隔离与逻辑隔离

物理隔离与逻辑隔离能够有效切断网络攻击途径，保障数据安全。物理隔离通过物理设备将不同网络完全分隔，如使用独立的服务器、存储设备和网络线路，使不同安全级别的网络之间不存在物理连接，防止外部网络的恶意渗透，常用于处理高度敏感数据的场景。逻辑隔离则通过 VLAN 划分、访问控制列表（ACL）等技术手段，在同一物理网络中构建多个相互隔离的虚拟网络，根据数据的重要性和安全性要求，限制不同虚拟网络之间的数据交互，实现对网络资源的灵活管控。两种隔离方式相互补充，既能从物理层面杜绝攻击，又能在逻辑层面优化网络安全架构，增强系统的安全性和防护能力。

2.3.4 做好数据备份与恢复

数据备份与恢复是应对数据丢失、损坏等风险的关键措施。制定详细的数据备份策略，明确备份数据的范围、频率和存储方式。对于重要数据，采用全量备份与增量备份相结合的方式，既能保证数据完整性，又能提高备份效率、节省存储空间。将备份数据存储在不同的物理位置，如本地备份与异地备份相结合，防止因自然灾害、硬件故障等原因导致数据全部丢失。同时，建立完善的数据恢复机制，定期进行恢复演练，确保在数据丢失或损坏时，能够快速、准确地恢复数据，最大限度减少业务中断时间和数据损失，保障企业和用户的正常运营与数据安全[2]。

3 计算机网络与信息安全系统的关键技术

3.1 防火墙技术

防火墙技术是计算机网络安全的第一道防线，通过监测、限制、更改跨越防火墙的数据流，尽可能地对外部屏蔽网络内部的信息、结构和运行状况，以此来实现网络的安全保护。从技术类型上，防火墙可分为包过滤防火墙、应用代理防火墙和状态检测防火墙。包过滤防火墙工作在网络层，依据数据包的源 IP 地址、目的 IP 地址、端口号等信息进行过滤，具有处理速度快的优点，但难以防范复杂攻击；应用代理防火墙在应用层对网络请求进行代理转发，能深入检查应用层数据，安全防护能力强，但存在性能损耗；状态检测防火墙结合前两者优势，在网络层监测数据包状态，同时对应用层协议进行分析，保障安全性的同时维持较高性能。在实际应用中，防火墙部署于内部网络与外部网络之间，通过设置访问控制规则，允许合法流量通过，拦截非法访问请求，防止外部网络的恶意入侵与攻击，保护内部网络安全。

3.2 入侵检测技术

入侵检测技术是一种主动的网络安全防护技术，通过对网络或系统中的关键信息（如网络流量、系统日志、用户行为等）进行实时收集、分析，检测是否存在违反安全策略的行为和被攻击的迹象。其主要分为基于主机的入侵检测系统（HIDS）、基于网络的入侵检测系统（NIDS）和分布式入侵检测系统（DIDS）。HIDS 安装在单个主机上，监测主机系统的日志、进程、文件等信息，能精准发现针对主机的攻击；NIDS 部署在网络关键节点，通过分析网络数据包来检测入侵行为，可实时监测整个网络流量；DIDS 则融合前两者优势，将多个 HIDS 和 NIDS 协同工作，实现对大规模、分布式网络环境的全面监测。入侵检测技术不仅能及时发现网络攻击，还可通过与防火墙等设备联动，在检测到攻击时自动阻断攻击源，防止攻击扩散。

3.3 加密技术

加密技术是保障数据机密性、完整性和可用性的核心技术，通过特定的算法将原始数据（明文）转换为不可读的密文形式，只有拥有对应密钥的用户才能将密文还原为明文。根据加密密钥的使用方式，加密技术分为对称加密和非对称加密。对称加密算法（如 AES、DES）使用相同的密钥进行加密和解密，加密速度快、效率高，但密钥管理复杂，存在密钥泄露风险；非对称加密算法（如 RSA）使用一对密钥（公钥和私钥），公钥公开用于加密，私钥保密用于解密，解决了密钥分发问题，常用于数字签名、密钥交换等场景，但加密速度较慢。在实际应用中，常采用对称加密与非对称加密相结合的方式，利用非对称加密进行密钥交换，再使用对称加密对大量数据进行加密传输，保障数据在存储和传输过程中的安全性。

3.4 访问控制技术

访问控制技术用于控制用户对网络资源的访问，确保只有授权用户能够访问特定的资源，防止非法用户的入侵和越权访问。其主要包括自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC）。DAC 允许资源所有者自主决定其他用户对资源的访问权限，灵活性高，但安全性相对较低；MAC 由系统强制对用户和资源进行分级，根据安全级别控制访问，安全性强，但缺乏灵活性；RBAC 则根据用户在组织中的角色分配权限，用户通过角色获得相应权限，便于管理和维护，适用于大型企业和复杂网络环境。在网络与信息安全系统中，访问控制技术通过身份认证、授权、访问审计等环节，实现对用户访问行为的全流程管控[3]。

结束语

计算机网络与信息安全系统的构建是一项复杂且持续的工程。从剖析网络面临的共享开放威胁、病毒攻击等风险，到实施物理环境、运行环境、软件数据环境的安全措施，再到应用防火墙、加密等关键技术，每一步都至关重要。随着网络技术的飞速发展，安全威胁也在不断演变，这要求我们持续关注技术动态，不断优化安全系统，提升防护能力，以确保计算机网络安全稳定运行，为数字时代的信息安全筑牢坚实防线。

参考文献

[1]张海,张焱.计算机网络与信息安全系统的建立与技术探究[J].煤炭技术,2013,32(04):242-244.

[2]于功成.计算机网络与信息安全系统的建立与技术分析[J].电子技术与软件工程,2015(07):212.

[3]付雪峰.关于计算机网络和信息安全系统的建立与技术策略研究[J].信息记录材料,2020,21(05):153-154.