网络安全维护中计算机安全技术分析

李　凯
内蒙古自治区大数据中心　内蒙古　呼和浩特　010090

摘　要：本文聚焦网络安全维护中的计算机安全技术。阐述关键计算机安全技术，包括身份认证与访问控制、加密与解密、防火墙与IDS、VPN与安全协议、恶意软件防护技术；分析系统安全与操作系统加固措施；探讨网络安全架构与防护策略，如网络拓扑设计、安全通信与协议优化、安全监控与应急响应，为网络安全维护提供全面的技术参考。

关键词：网络安全；计算机安全技术；身份认证；加密解密；防火墙

引言：在数字化时代，计算机技术飞速发展，网络应用广泛普及，网络安全问题愈发凸显。计算机安全技术作为网络安全维护的核心支撑，涵盖身份认证、加密解密、防火墙、恶意软件防护等多个方面。系统安全与操作系统加固是保障计算机稳定运行的基础，网络安全架构与防护策略则为网络环境筑牢安全防线。深入分析这些计算机安全技术，对于有效应对网络安全威胁、维护网络空间的安全稳定具有重要意义。

1 关键计算机安全技术

1.1 身份认证与访问控制

身份认证技术是保障系统安全的首道防线。密码学作为传统且广泛应用的认证方式，通过设置复杂字符组合的密码，结合哈希函数对密码进行加密存储，验证时比对哈希值，防止密码在传输和存储过程中被窃取。生物识别技术凭借人体独特的生理或行为特征实现精准认证，指纹识别利用指纹纹路的唯一性，虹膜识别依靠虹膜的复杂纹理结构，这些技术具有不可复制性，极大提升了认证的安全性。多因素认证结合多种验证方式，如密码加短信验证码、生物特征加硬件令牌，即使某一因素被破解，其他因素仍能保障认证安全。访问控制模型决定用户对系统资源的访问权限。自主访问控制（DAC）允许资源所有者自行设定访问权限，灵活性高，但可能因用户误操作或恶意设置导致权限失控。强制访问控制（MAC）依据安全标签对用户和资源分级，严格限制不同级别间的访问，常用于对安全性要求极高的军事和政府系统。基于角色的访问控制（RBAC）根据用户角色分配权限，如企业中财务角色拥有资金操作权限，普通员工仅能访问基础办公资源，简化权限管理的同时降低权限滥用风险。

1.2 加密与解密技术

加密与解密技术保障数据的保密性和完整性。对称加密算法使用同一密钥进行加密和解密，AES（高级加密标准）以其高效性和安全性广泛应用于数据存储和传输，如数据库中敏感信息的加密[1]。非对称加密算法采用公钥加密、私钥解密的方式，RSA算法常用于数字证书和密钥交换，公钥公开用于加密数据，私钥由持有者妥善保管用于解密，确保数据仅能被授权者访问。哈希函数将任意长度的数据转换为固定长度的哈希值，常用于验证数据完整性。不同数据生成的哈希值具有唯一性，若数据被篡改，哈希值将发生变化。数字签名结合哈希函数与非对称加密，发送方用私钥对数据哈希值签名，接收方用公钥验证，确保数据来源可靠且未被篡改，在电子合同签署等场景中发挥关键作用。

1.3 防火墙与入侵检测系统（IDS）

防火墙作为网络安全的屏障，存在多种类型。包过滤防火墙基于IP地址、端口号等网络层信息对数据进行筛选，允许或拒绝特定数据包通过，效率高但难以抵御复杂攻击。状态检测防火墙跟踪网络连接状态，不仅检查数据包信息，还记录连接上下文，能有效防范基于连接的攻击。应用层防火墙深入分析应用层协议，如HTTP、FTP，对应用数据进行过滤和控制，防止恶意代码注入和非法操作。入侵检测系统实时监控网络和系统活动。基于签名的入侵检测方法将已知攻击特征编写为规则库，通过比对网络流量和系统日志与规则库，发现匹配的攻击行为。基于异常的入侵检测则建立正常行为模型，当检测到与模型偏差较大的行为时，判断为潜在攻击，能发现未知攻击，但误报率相对较高。

1.4 虚拟专用网络（VPN）与安全协议

虚拟专用网络（VPN）在公共网络上构建安全通道。IPsec（互联网协议安全）VPN在网络层建立安全连接，通过加密和认证机制保护数据传输，常用于企业分支机构之间的互联。SSL/TLSVPN在应用层实现安全访问，用户通过Web浏览器即可接入，适用于远程办公场景。VPN技术通过隧道封装，隐藏真实网络地址和数据

内容，防止数据被窃取和篡改。安全协议为网络通信提供安全保障。WPA3（Wi-Fi保护访问3）作为新一代无线网络安全协议，增强了数据加密强度和身份认证机制，抵御暴力破解和密钥窃取。TLS1.3（传输层安全1.3）优化了握手过程，减少数据传输延迟，提高加密性能，广泛应用于HTTPS网站和网络服务，保障数据在传输过程中的安全性。

1.5 恶意软件防护技术

恶意软件威胁着计算机系统安全。病毒依附于正常程序，通过文件传播，修改或破坏文件内容。蠕虫利用系统漏洞自主传播，消耗网络资源导致系统瘫痪。木马伪装成正常程序，窃取用户敏感信息。检测恶意软件需结合特征码检测和行为分析，特征码检测比对已知恶意软件的代码特征，行为分析则监控程序运行行为，识别异常操作。沙箱技术为程序提供隔离的运行环境，恶意软件在沙箱内的操作被限制，无法对真实系统造成损害。通过分析程序在沙箱内的行为，如文件读写、网络连接等，判断其是否为恶意软件[2]。行为分析技术结合机器学习算法，不断学习新的恶意行为模式，提升对未知恶意软件的检测能力，有效保障计算机系统安全。

2 系统安全与操作系统加固

2.1 操作系统安全机制

操作系统安全机制通过用户权限管理与审计确保系统访问可控。用户权限采用分级策略，将用户划分为管理员、普通用户等不同角色，管理员拥有系统配置、软件安装等高级权限，普通用户仅能访问授权资源。权限分配遵循最小化原则，仅赋予用户完成任务所需的最低权限，降低权限滥用风险。审计功能则记录用户操作日志，包括登录时间、文件访问、系统配置修改等行为，便于追溯异常操作来源，及时发现违规行为或安全事件。内存保护机制保障系统运行稳定与数据安全。内存地址空间划分不同区域，对内核空间与用户空间进行隔离，防止用户程序非法访问内核数据。采用地址随机化技术，每次系统启动时随机分配内存地址，增加攻击者利用缓冲区溢出等漏洞的难度。代码完整性校验通过哈希算法对系统核心代码进行校验，一旦检测到代码被篡改，立即触发安全警报并阻止异常代码执行，确保操作系统内核与关键程序的完整性。

2.2 安全配置与漏洞修复

操作系统安全配置从最小化安装与端口管理入手。最小化安装仅保留必要的组件和服务，减少潜在攻击面。例如，服务器操作系统仅安装与业务相关的服务，关闭不必要的功能模块。端口管理严格控制开放端口，仅开启业务必需的端口，如Web服务器仅开放80和443端口，通过防火墙对端口访问进行过滤，限制非法的网络连接请求。补丁管理与自动化更新是修复系统漏洞的关键。操作系统厂商定期发布安全补丁修复已知漏洞，及时安装补丁可有效抵御利用漏洞的攻击。自动化更新机制自动检测、下载并安装补丁，避免因人为疏忽导致补丁滞后。更新前进行兼容性测试，防止补丁引发系统故障，确保系统在修复漏洞的同时保持稳定运行。

2.3 容器与虚拟化安全

容器隔离技术确保容器化应用的安全运行。Docker通过命名空间（Namespace）和控制组（Cgroup）实现容器间资源隔离与权限分离，每个容器拥有独立的文件系统、网络和进程空间，避免容器间资源冲突与数据泄露。Kubernetes作为容器编排平台，进一步强化安全管理，通过网络策略控制容器间的网络通信，限制容器访问范围，同时提供密钥管理功能，保障敏感数据安全。虚拟化环境面临漏洞与逃逸攻击风险，需采取针对性防范措施[3]。虚拟化漏洞可能导致虚拟机突破隔离边界，访问宿主机或其他虚拟机资源。通过定期更新虚拟化软件补丁修复已知漏洞，同时对虚拟机进行安全加固，限制不必要的特权操作。采用内存隔离、设备模拟限制等技术，防止恶意虚拟机通过硬件接口发起攻击，确保虚拟化环境中各虚拟机安全独立运行，避免安全事件扩散。

3 网络安全架构与防护策略

3.1 网络拓扑与分段设计

微分段与零信任网络架构重塑网络安全边界。微分段通过将网络细化为高度颗粒化的安全单元，每个单元对应特定业务功能或用户群体，如财务结算、客户数据管理等系统均独立成段。通过为各分段设置精准访问控制策略，仅允许必要业务流量通过，可有效遏制攻击在网络中的横向扩散。例如，若办公终端被入侵，攻击者因难以突破分段边界，将无法接触核心业务数据。零信任网络架构摒弃了传统"内网即安全"的观念，所有网络访问请求均需经过严格身份验证与权限审查。从用户登录的多因素认证，到设备接入的合规性检查，再到基于用户角色、行为模式和设备状态的动态权限分配，每个环节均确保只有授权设备与用户能够访问资源。例如，员工即使身处内网，每次访问核心数据库时仍需重新认证，且权限会根据当前操作行为动态调整。冗余与容错机制是保障网络稳定运行的基础。网络拓扑设计中，冗余链路部署已成为标准配置，核心交换机之间通过链路聚合技术实现多条物理连接，既可同时承载流量以提升带宽，又能在链路故障时自动切换，确保数据传输不中

断。关键网络设备采用双机热备或集群模式，主设备故障时，备用设备可迅速接管业务，保障服务连续性。分布式网络架构通过将负载分散至多个节点，使部分节点遭受攻击或失效时，整个网络仍能维持基本功能，显著增强抗风险能力。

3.2 安全通信与协议优化

加密通道与数据传输保护是确保信息安全的关键手段。虚拟专用网络（VPN）技术通过在公共网络上构建加密隧道，实现安全的数据传输。IPsecVPN在网络层对数据进行加密封装，适用于企业分支机构间的安全互联；SSL/TLSVPN则在应用层建立加密连接，方便远程办公用户安全访问内部资源。端到端加密技术更进一步，数据仅在发送端与接收端进行解密，即使通信链路被截取，中间节点也无法获取明文内容，特别适用于金融交易、机密文件传输等场景。数据传输过程中引入完整性校验机制，利用哈希算法生成数据摘要，接收端通过比对摘要验证数据是否完整，有效防止数据被篡改[4]。协议安全增强为网络通信构筑了更坚固的防线。HTTP/3协议基于QUIC（快速UDP互联网连接）协议，从多个方面提升了网络性能与安全性。QUIC协议在传输层集成加密功能，采用TLS1.3加密标准，确保数据传输的机密性与完整性；其多路复用技术解决了HTTP/2协议的队头阻塞问题，实现了更高效的数据传输；快速握手机制大幅缩短了连接建立时间，降低了延迟。除了新兴协议的应用，传统网络协议也在不断升级优化，如SSH协议增加了双因素认证机制，FTP协议逐步被支持加密传输的FTPS、SFTP协议取代，有效填补了协议层面的安全漏洞。

3.3 安全监控与应急响应

日志管理与安全信息事件管理（SIEM）系统构成了网络安全监控的中枢神经。网络设备、服务器、应用程序产生的日志记录着系统运行的各类信息，通过集中式日志管理系统，这些分散的日志数据被统一收集、存储与管理。SIEM系统运用预设的规则引擎和机器学习算法，对海量日志数据进行实时分析，能够快速识别异常行为与安全事件。例如，系统可以检测到短时间内大量的失败登录尝试、异常的文件访问模式、非授权的网络连接等可疑活动，并及时发出警报。SIEM系统具备关联分析能力，能够整合多个日志源的信息，还原安全事件的全貌，为安全人员调查取证提供有力支持。应急响应流程与恢复策略是网络安全防护的最后一道屏障。一套完善的应急响应机制包含多个关键环节：安全事件发生后，首先进行快速确认与影响评估，通过分析系统日志、监控数据，判断事件的性质与严重程度；随后立即启动响应程序，隔离受影响的网络区域，阻断攻击传播路径，同时开展取证工作，保存攻击痕迹与相关数据；进入恢复阶段后，安全团队需清理恶意代码、修复系统漏洞，并逐步恢复业务系统运行。为确保应急响应机制的有效性，企业需定期开展应急演练，模拟各类安全事件场景，检验和优化响应流程，提升安全团队的实战能力与协同效率，从而在真实安全事件发生时，将损失降至最低。

结束语

网络安全维护中的计算机安全技术，是保障信息系统安全稳定运行的关键。从关键安全技术到系统安全加固，再到网络安全架构与防护策略，各环节相互关联、协同作用。随着网络技术的不断发展，安全威胁也将持续演变。需持续关注新技术、新威胁，不断优化和完善安全防护体系，提升安全防护能力，以应对日益复杂的网络安全挑战，为数字时代的信息安全保驾护航。

参考文献

[1]钟建坤.大数据时代信息通信网络安全管理策略[J].数字通信世界,2022（8）:173-175.

[2]王永范.计算机网络安全技术在网络维护中的应用[J].信息系统工程,2023(09):43-46.

[3]王宇.网络维护中计算机网络安全技术的应用策略探究[J].科技创新与应用,2022,12(33):185-188.

[4]周燕彬.网络安全维护中计算机网络安全技术的应用探讨[J].科技创新与生产力,2023(1):75-77.