计算机应用中的网络安全防护研究

魏　栗
石家庄市城市照明管护中心　河北　石家庄　050000

摘　要：计算机应用面临系统与硬件、应用与数据、网络连接等多重安全威胁。为应对这些威胁，需综合运用边界防护、数据与身份防护、终端防护等核心技术，搭建包含基础防护层级、防护策略与管理、防护效果评估与优化的防护体系。通过多层级、全方位的防护措施，提升计算机应用的安全性，确保其稳定运行与数据安全，适应不断变化的网络安全环境。

关键词：计算机应用；网络安全；防护技术；防护体系；威胁分析

引言：数字化时代，计算机应用渗透至各领域，成为推动社会发展的关键力量。其稳定运行依赖安全环境，但系统漏洞、恶意攻击等威胁频发，严重威胁应用安全。构建完善的网络安全防护体系，成为保障计算机应用安全运行的迫切需求。本文分析计算机应用面临的安全威胁，探讨核心防护技术，提出防护体系搭建方案，为提升计算机应用安全性提供参考。

1 计算机应用中的常见安全威胁

1.1 系统与硬件威胁

系统与硬件是计算机应用运行的基础载体，其安全隐患直接影响应用稳定运行，甚至致使功能失效或数据泄露。操作系统漏洞是系统层面主要威胁，因设计时需兼顾多种功能与设备兼容，复杂代码编写和逻辑设计易出现缺陷或漏洞。部分漏洞在系统发布初期未被察觉，随应用场景拓展和技术迭代逐渐暴露。计算机应用依赖存在漏洞的操作系统时，攻击者可借此绕过安全验证，获取系统控制权，篡改或破坏应用程序，导致应用无法正常服务，敏感信息易被窃取。硬件设备隐患中，固件问题较为典型。固件是嵌入硬件的程序，主板、硬盘、网卡等均依靠固件运行。若固件开发缺乏严格安全校验，易存在漏洞[1]。攻击者利用这些漏洞，修改固件程序改变硬件运行逻辑。例如，硬盘固件问题可能导致存储数据无法读取，应用关键数据丢失，中断应用运行；网卡固件漏洞可能导致网络数据传输泄露，应用交互数据被截取。此外，硬件长期使用会出现部件老化或故障，如内存故障使应用运行数据出错，CPU性能下降减缓应用处理速度，这些问题虽非人为攻击，仍影响应用稳定性与安全性。

1.2 应用与数据威胁

应用程序是计算机应用实现功能的核心，数据是应用处理的关键对象，二者安全威胁直接关乎应用功能价值与数据安全。应用程序缺陷多源于开发阶段不规范操作。应用开发历经需求分析、代码编写、测试等环节，若开发人员缺乏安全意识，未遵循安全编码规范，易留下输入验证不严格、权限控制不完善等隐患。这些缺陷使应用成为安全薄弱点，攻击者可利用输入验证漏洞注入恶意代码，篡改应用逻辑，导致应用功能异常；权限控制缺陷可能让未授权用户获取高级权限，修改应用配置或删除关键文件，破坏应用完整性。数据传输安全风险源于网络环境不确定性。应用处理数据时，常需在不同设备或系统间传输，如用户数据传输至服务器处理后反馈至用户设备。数据传输经过多个网络节点，若未采取安全措施，易被非法节点拦截。拦截数据可能被查看或篡改，导致接收方获取虚假数据，影响应用基于数据的判断或操作。数据存储安全风险与存储介质和方式相关。应用数据多存储在硬盘、U盘、云存储等介质中，若存储介质未加密，一旦丢失或被非法访问，数据可能被窃取或删除。比如，应用用户信息存储在未加密硬盘分区，硬盘被他人获取后，用户信息易被读取，造成隐私泄露，影响应用用户信任度。

1.3 网络连接威胁

计算机应用多依赖网络连接实现数据交互与功能拓展，网络连接安全威胁直接影响数据传输安全与应用可用性。网络协议漏洞是网络层面重要隐患，网络协议是设备间数据交换规则，如TCP/IP协议族是互联网常用协议。部分早期协议设计时侧重传输便捷性与效率，未充分考虑安全，导致存在安全缺陷。随网络技术发展，这些漏洞逐渐显现，攻击者可利用漏洞发起攻击，如伪装合法设备与应用连接获取传输数据，或发送异常数据包导致应用网络模块崩溃，中断应用网络功能。不安全接入是用户使用应用时易遭遇的威胁，公共网络场景下问题尤为突出。公共WiFi为满足大量用户接入，通常

未采取严格身份认证与数据加密，网络环境开放且缺乏监管。用户在公共网络使用应用时，应用与服务器传输数据易被其他用户截取。此外，公共网络中可能存在攻击者搭建的虚假接入点，伪装合法公共网络。用户误连后，应用发送的所有数据会传输至攻击者设备，攻击者可查看或篡改数据，甚至植入恶意程序，监控用户操作获取敏感信息。家庭或企业内部网络若未配置合理防护，也可能面临非法接入风险，攻击者通过破解密码或利用设备漏洞接入网络，对应用发起攻击。

2 核心网络安全防护技术

2.1 边界防护技术

边界防护技术是计算机应用与外部网络交互的第一道安全屏障，通过构建网络边界防护规则，阻挡非法访问与恶意攻击，保障应用运行环境的基础安全。防火墙作为边界防护的核心技术，基础作用是依据预设安全策略对网络流量进行过滤与管控[2]。它能识别网络数据的来源地址、目标地址、传输协议及端口信息，按预设规则判断数据是否允许通过。外部设备试图与应用所在内部网络建立连接时，防火墙会检查连接请求的来源IP与端口，符合规则则放行数据传输，未授权请求则直接阻断，避免外部非法数据干扰应用运行。入侵检测系统通过实时监测网络流量与系统行为，及时发现潜在攻击并发出告警。它持续收集网络数据传输信息与应用运行日志，对比已知攻击特征库与异常行为模式，识别入侵迹象。网络中出现异常数据包传输、频繁端口扫描或应用异常调用时，入侵检测系统会触发告警机制，通知管理人员关注风险，为安全处置争取时间。入侵防御系统在入侵检测基础上增加主动阻断功能，既能识别攻击行为，又能自动采取防护措施阻止攻击继续。检测到外部设备向应用发起恶意数据包攻击时，可直接切断攻击连接或修改网络规则屏蔽攻击源IP，避免攻击对应用造成实际损害。这类边界防护技术相互配合，从“过滤-检测-防御”三个层面构建网络边界安全防线，减少外部威胁对应用的直接冲击。

2.2 数据与身份防护技术

数据与身份防护技术聚焦计算机应用的核心资产与访问权限管控，通过保障数据安全与规范身份验证，防止敏感信息泄露与未授权访问。数据加密技术通过特定算法将原始数据转换为不可直接读取的密文，仅掌握解密密钥的授权主体能将密文还原为明文。在计算机应用中，数据加密可应用于数据传输与存储两个关键环节。数据传输时，加密技术能保护应用与服务器、用户设备与应用间交互的数据，即使数据被非法截取，截取者因缺乏解密密钥无法获取实际内容，避免传输环节信息泄露。数据存储时，加密技术可对应用存储在硬盘、云服务器等介质中的敏感数据进行加密，即使存储介质丢失或被非法访问，加密后的数据也难以被破解，保障存储安全性。身份认证技术通过验证用户或设备身份信息，确保仅授权主体能访问应用及相关资源。密码认证是最基础的方式，用户需输入预设密码，应用系统通过比对密码正确性判断身份合法性。但单一密码认证存在安全风险，密码若被窃取或破解，未授权者可能冒充合法用户访问应用。多因素认证在密码认证基础上增加额外验证维度，结合用户拥有的物品（如手机验证码）、自身生物特征（如指纹、面部识别）等进行验证。用户输入正确密码后，还需通过手机接收验证码输入系统，或通过指纹识别完成二次验证，所有环节通过才能成功访问应用。这种多维度认证大幅提升身份验证安全性，降低未授权访问风险，为应用访问权限管控提供更可靠保障。

2.3 终端防护技术

终端防护技术针对计算机应用运行的终端设备构建防护体系，通过管控终端状态与防御恶意程序，保障应用在终端层面安全。终端安全管理技术统一管控终端硬件、软件及运行状态，监测硬盘、内存等硬件状态，及时发现故障或异常连接；管理软件安装与运行，限制未授权软件，防止恶意软件或有漏洞的软件威胁应用；还能统一配置安全参数，如设置系统补丁更新策略、规范网络连接设置，确保终端符合安全要求。恶意代码防护技术识别与清除终端中的恶意程序，阻止其破坏应用与窃取数据。恶意代码包括病毒、木马等，通过感染文件、伪装正常软件进入终端[3]。防护技术通过特征码检测比对文件与已知恶意代码特征，清除含恶意特征的文件；通过行为分析监测程序运行，识别未授权读取数据、修改应用配置等恶意行为并拦截。终端中出现修改应用关键文件的程序时，技术会识别异常并阻止操作，减少恶意程序攻击，保障应用完整性与稳定性。

3 网络安全防护体系搭建

3.1 基础防护层级

基础防护层级是网络安全防护体系的核心框架，通过覆盖物理安全、网络安全、主机与应用安全的简单架构，为计算机应用构建多层级安全防护基础。物理安全作为底层支撑，聚焦应用运行所需物理环境与硬件设备的安全。它管控机房人员进出权限，避免未授权人员接触服务器、网络设备等关键硬件；同时为服务器配备防尘、防潮、防电磁干扰装置，防止硬件因环境或人为因素故障，保障应用运行的硬件基础稳定。网络安全承担

内外网络连接的安全管控职责，通过防护机制阻挡外部威胁进入内部网络。这一环节采用网络分区策略，将内部网络划分为办公区域、核心业务服务器区域等安全区域，区域间设访问控制规则，限制随意数据交互，减少单一区域被攻击后的风险扩散。同时部署防火墙、入侵防御系统，实时监测与过滤网络流量，拦截非法访问请求与恶意数据包，保障网络数据传输安全，为应用提供安全的网络环境。主机与应用安全针对应用运行的核心载体，聚焦主机系统与应用程序防护。主机安全方面，对操作系统进行安全加固，关闭不必要的服务与端口，及时安装补丁修复漏洞，防止攻击者入侵；同时配置主机访问权限，明确用户操作权限，避免未授权用户修改配置或获取敏感信息。应用安全方面，开发阶段引入安全测试排查缺陷与隐患；运行阶段监测应用状态，及时发现异常资源占用、错误日志等行为，避免应用因安全问题中断或泄露数据。

3.2 防护策略与管理

防护策略与管理是防护体系有效运行的保障，通过制定日常安全规则与培养人员安全意识，将防护融入应用使用全流程。日常安全规则结合应用特点与需求，形成可执行规范。数据管理方面，明确数据分类标准，对不同敏感数据制定存储、传输与销毁规则，如敏感数据加密存储、传输用安全协议、废弃数据用专业工具删除，防止泄露。设备管理方面，规范终端使用流程，如设复杂登录密码并定期更换，禁止接入不明存储介质，防止恶意软件侵入。人员安全意识培养是关键环节，通过提升认知减少人为操作失误风险[4]。开展定期安全培训，讲解网络钓鱼、恶意代码攻击等威胁，介绍辨别虚假邮件、可疑文件的方法。同时通过案例让人员了解不安全操作后果，如点击可疑链接致终端入侵、用弱密码致账号被盗。此外制定考核机制，定期检验人员对安全规则的掌握程度，督促其将规范融入日常，形成良好习惯，从人员层面支撑防护体系。

3.3 防护效果评估与优化

防护效果评估与优化是防护体系持续完善的重要环节，通过明确评估维度与优化方向，确保体系适应应用安全需求。评估维度围绕核心功能设定，全面衡量运行效果。威胁拦截率是重要维度，通过统计对已知威胁的拦截数量，判断防护技术与策略的阻挡能力，如防火墙拦截非法访问、恶意代码防护识别清除恶意程序的情况。漏洞修复时效是关键维度，记录漏洞发现至修复时间，评估体系对隐患的响应速度，避免漏洞长期存在给攻击者可乘之机。此外评估体系资源占用，判断对应用性能的影响，如是否致应用变慢、终端资源消耗过高，确保安全与应用使用兼顾。基于评估结果的优化需针对问题制定措施，提升体系安全性与适应性。若某类威胁拦截率低，分析威胁特征与防护不足，补充技术或更新策略，如针对新型恶意代码升级防护特征库，增强识别能力。若漏洞修复时效不达标，优化管理流程，建立高效发现与修复机制，如增加扫描频率、明确修复责任与时间，加快修复速度。若资源占用过高，调整防护配置，选轻量化方案，在保效果的同时降低对应用性能的影响。通过持续评估与优化，使防护体系应对变化的威胁，为应用提供长期稳定的安全保障。

结束语

计算机应用中的网络安全防护是系统性工程，需综合技术、管理与策略等多方面因素。通过构建多层级防护体系，结合边界、数据、终端等防护技术，并强化日常安全管理与人员意识培养，可显著提升应用安全性。未来，随着网络安全威胁的不断演变，需持续优化防护体系，以适应新的安全挑战，确保计算机应用的安全稳定运行。

参考文献

[1]张敏.计算机应用中的网络安全防护研究[J].中国新通信,2024,26(23):41-43.

[2]周运科.大数据背景下计算机网络安全与防护措施[J].数字通信世界,2024,(11):95-97.

[3]刘明珍.计算机应用中网络安全防护体系构建的分析[J].数字技术与应用,2024,42(08):75-77.

[4]魏恩志.计算机应用中网络安全防护体系构建研究[J].石河子科技,2022,(06):30-32.