计算机网络工程安全与病毒防护

雷趁喜
石河子工程职业技术学院　新疆　石河子　832000

摘　要：随着计算机网络技术的飞速发展，网络已成为社会运转的重要基础设施，但网络安全问题也日益凸显。本文围绕计算机网络工程安全与病毒防护展开研究，明确了网络工程安全的定义与范畴，涵盖物理、数据、应用等层面，分析DDoS攻击、SQL注入等常见威胁。其次阐述计算机病毒的定义、分类、传播机制及危害。在此基础上，构建网络工程安全防护体系，包括层次化设计、安全策略与管理制度及性能平衡机制。最后探讨病毒防护的传统与新型技术，以及终端与网络层的协同机制。研究旨在为网络安全防护提供理论与技术参考，提升网络系统抵御威胁的能力。

关键词：计算机；网络工程安全；病毒防护

引言：计算机病毒与各类攻击手段对网络系统的完整性、保密性和可用性构成严重威胁，影响个人权益与社会稳定。当前网络安全防护面临攻击手段多样化、病毒变异加速等挑战，亟需构建全面有效的防护体系。本文立足网络工程安全基础，深入分析病毒特性与防护技术，探索多层次协同防护机制，为应对网络安全威胁提供系统性解决方案，具有重要的理论与实践意义。

1 计算机网络工程安全基础

1.1 定义与范畴

计算机网络工程安全是指通过技术手段与管理策略，保障计算机网络系统在运行过程中免受各类威胁干扰，确保网络基础设施、数据信息及应用服务的完整性、保密性和可用性。其范畴涵盖以下多个相互关联的层面。（1）物理安全是基础，涉及网络硬件设备通信线路及机房环境的防护，需防范设备被盗、线路被破坏、环境异常等风险；数据安全是核心，聚焦数据在产生、传输、存储、使用全生命周期的保护，包括防止数据泄露、篡改、丢失，同时需满足合规性要求；（2）应用安全针对网络中的软件系统，旨在抵御因程序漏洞引发的安全风险，保障应用程序按预期功能稳定运行。（3）网络安全还涉及网络拓扑结构设计的合理性、访问控制机制的有效性，以及人员操作规范等管理层面的内容，各层面协同形成完整的安全防护体系。

1.2 安全威胁分析

常见的网络攻击手段具有技术隐蔽性强、攻击路径多样的特点，对网络安全构成持续性挑战。DDoS攻击通过控制大量傀儡机向目标服务器发送海量无效请求，耗尽服务器带宽与资源，导致合法用户无法正常访问，其核心是利用资源耗尽原理破坏网络服务的可用性；SQL注入攻击针对数据库应用程序的漏洞，通过在输入字段插入恶意SQL语句，非法获取、篡改或删除数据库中的敏感信息，本质是利用程序对用户输入验证不足的缺陷；跨站脚本攻击则利用Web应用对用户输入过滤不严的漏洞，将恶意脚本注入网页，当其他用户访问该页面时，脚本被执行，可能导致用户cookie被盗、会话劫持或虚假信息展示，其攻击目标直接指向应用使用者的终端安全[1]。

2 计算机病毒概述

2.1 病毒定义与分类

计算机病毒是一段能够自我复制且具有破坏性的计算机程序代码，它通常依附于其他程序而存在，在特定条件下被激活后，会对计算机系统造成损害。与计算机病毒容易混淆的恶意软件还有蠕虫和木马。计算机病毒主要侧重于自我复制和传播，往往需要寄生在宿主程序中，通过感染其他文件来扩散。蠕虫则是一种独立的恶意程序，它不需要寄生在宿主文件中，能够利用网络协议自主传播，通过网络快速蔓延，大量占用系统资源，导致网络拥塞甚至瘫痪。木马则是一种伪装成合法程序的恶意软件，它不会自我复制和传播，而是通过欺骗用户的方式，在用户不知情的情况下植入系统，为攻击者提供远程控制通道，窃取用户信息或执行其他恶意操作。

2.2 病毒传播机制

计算机病毒的传播途径多种多样，网络是其最为主要的传播渠道之一。在网络环境中，病毒可以通过漏洞利用、网络共享等方式迅速传播到其他计算机。一些病毒会扫描网络中存在漏洞的计算机，并利用这些漏洞进行感染和传播。邮件也是病毒传播的重要途径，病毒可以隐藏在邮件的附件中，当用户打开附件时，病毒就会被激活并感染计算机。可移动存储设备如U盘、移动硬盘

等，由于其便携性和通用性，也成为病毒传播的常见媒介。当带有病毒的可移动存储设备插入计算机时，病毒会自动运行并感染系统文件，进而传播到其他设备。

2.3 病毒危害评估

计算机病毒对计算机系统和用户造成的危害是多方面的。在系统性能方面，病毒会占用大量的系统资源，如CPU、内存等，导致计算机运行速度变慢，甚至出现死机、重启等现象。对于数据完整性，病毒可能会篡改、删除或破坏系统中的重要文件和数据，造成数据的丢失或损坏，给用户带来巨大的损失。在用户隐私方面，一些病毒具有窃取用户信息的功能，如账号密码、银行卡信息等，这些信息一旦被窃取，用户的财产安全和个人隐私将面临严重威胁[2]。

3 网络工程安全防护体系构建框架

3.1 防护体系的层次化设计

网络工程安全防护体系的层次化设计通过以下物理层、网络层、应用层、数据层的逐级防护，形成纵深防御机制。（1）物理层作为防护体系的底层支撑，聚焦于网络基础设施的实体安全，包括机房环境的门禁控制、监控系统部署、设备防电磁干扰设计以及通信线路的物理隔离。（2）网络层防护针对数据传输过程中的安全风险，通过部署防火墙、入侵检测系统、虚拟专用网络等技术，实现对网络流量的实时监控与过滤。该层次需构建动态访问控制规则，限制不同网络区域间的非必要通信，并对异常流量进行快速识别与阻断，确保数据在传输路径中的完整性与保密性。（3）应用层防护聚焦于各类软件应用的安全运行，通过代码审计、漏洞扫描、应用防火墙等手段，消除应用程序在开发与运行过程中存在的安全缺陷。该层次需建立应用程序的全生命周期安全管理机制，从需求分析阶段嵌入安全设计，在测试阶段强化漏洞检测，在运维阶段实施实时监控，防止因应用程序漏洞引发的数据泄露或服务中断。（4）数据层作为防护体系的核心环节，围绕数据的产生、传输、存储、使用全流程构建安全机制。通过数据加密、脱敏、备份与恢复等技术，确保数据在任何状态下的保密性与完整性。数据层需建立严格的权限管理体系，依据数据敏感级别划分访问权限，并对数据操作进行全程审计，实现数据可追溯。

3.2 安全策略与管理制度

安全策略与管理制度通过规范化的制度设计与流程管控，将技术防护转化为常态化的安全管理能力。具体如下：（1）访问控制制度。需明确主体与客体的权限映射关系，采用最小权限原则分配访问权限，并实施动态权限调整机制。同时建立严格的身份认证体系，结合多因素认证、单点登录等技术，确保访问主体的合法性与唯一性。（2）应急响应制度。旨在提升网络系统应对安全事件的处置能力，要构建涵盖预案制定、事件监测、应急处置、事后复盘的全流程机制。预案制定阶段需明确各类安全事件的分级标准与处置流程，明确各部门的职责分工；事件监测阶段依托安全监控系统实现对异常行为的实时预警；应急处置阶段按照预案快速实施隔离、止损、恢复等操作；事后复盘阶段需对事件原因进行深入分析，形成改进方案并更新防护策略。（3）人员安全意识培养。建立分层分类的安全培训体系。针对技术人员开展专业安全技能培训，提升其漏洞检测与应急处置能力；针对普通用户开展基础安全知识教育，强化密码管理、钓鱼邮件识别等日常安全习惯；针对管理层开展安全责任教育，推动安全管理融入业务决策。

3.3 安全防护与网络性能的平衡机制

安全防护与网络性能的平衡需在保障安全的前提下，最大限度降低对网络运行效率的影响，避免过度防护导致的资源浪费或服务延迟，具体如下：（1）技术优化层面，选择具备高性能的安全设备与算法，例如采用硬件加速的防火墙、基于并行计算的入侵检测系统，减少安全处理对网络带宽的占用。同时对安全策略进行动态优化，通过流量特征分析精简访问控制规则，避免冗余规则导致的处理延迟。（2）资源调度机制。建立基于网络负载的动态资源分配策略。在网络高峰期，可适当调整安全检测的精度与频率，优先保障核心业务的正常运行；在网络空闲期，启动深度检测模式，全面扫描潜在安全风险。通过虚拟化、云计算等技术实现安全资源的弹性扩展，根据实际需求动态分配计算、存储资源，避免资源闲置或过载。（3）架构设计层面。采用分布式防护架构，将安全功能下沉至网络边缘节点，实现就近防护与流量清洗，减少核心网络的处理压力。通过构建安全与业务的协同调度机制，将安全策略与业务需求相匹配，例如对实时性要求高的业务采用轻量化安全检测，对敏感数据传输采用高强度加密，实现安全防护的差异化实施[3]。

4 计算机病毒防护的关键技术与应用

4.1 传统病毒防护技术

传统病毒防护技术是应对病毒威胁的基础手段，通过对病毒特征、行为模式的解析构建防御体系，具体如下：（1）特征码检测技术。以病毒的独特代码片段为识别依据，通过建立庞大的特征码数据库，对文件或内存中的数据进行比对，从而快速识别已知病毒。其核心在

于特征码的精准提取与数据库的实时更新，依赖对病毒样本的持续收集与分析，能够在短时间内对常见病毒做出响应。（2）启发式扫描技术。突破了对已知病毒的依赖，通过预设的可疑行为规则库，对程序的指令序列、代码结构进行静态分析，判断其是否存在潜在的恶意意图。该技术不局限于特定特征，可对变异病毒或未知病毒进行初步筛查，但其检测精度受规则库完善程度影响，易出现误报或漏报。（3）行为监控技术。聚焦于程序运行时的动态行为，通过对进程创建、文件操作、注册表修改、网络连接等行为的实时追踪，识别病毒的典型破坏动作。它能够在病毒触发恶意行为的早期进行拦截，弥补了静态检测对隐藏性病毒的防御不足，同时可与其他技术结合形成多层防御，但对系统资源的消耗相对较高，需在监控粒度与运行效率间寻求平衡。

4.2 新型防护技术

新型防护技术依托前沿科技发展，针对病毒变异加速、形态多样化的特点，构建更具适应性的防御机制，主要技术有：（1）沙箱技术。通过创建隔离的虚拟执行环境，将可疑程序置于其中运行，观察其在封闭系统内的行为表现，从而判断是否具有恶意属性。这种技术能够避免可疑程序对真实系统造成破坏，同时可完整记录病毒的触发条件与破坏路径，为后续防御策略优化提供依据，尤其适用于对未知病毒的分析与检测。（2）机器学习检测技术。通过算法模型对海量病毒样本与正常程序数据进行训练，使系统具备自主识别病毒的能力。它能够从数据中挖掘病毒的隐藏特征与行为模式，对变异病毒或新型病毒做出快速响应，减少对人工特征码更新的依赖。随着深度学习等算法的应用，该技术的检测精度与泛化能力不断提升，但需持续输入高质量的训练数据以应对病毒的动态演化。（3）区块链溯源技术。利用分布式账本的不可篡改特性，记录病毒样本的传播路径、变异历史及检测记录。通过构建病毒信息共享链，可实现不同防护系统间的信息同步，提升对病毒溯源的效率与准确性。区块链的去中心化架构能避免单点数据篡改风险，为跨机构、跨区域的病毒协同防御提供可信的数据支撑，推动病毒防护从个体防御向协同防御升级。

4.3 终端与网络层病毒防护的协同机制

终端与网络层病毒防护的协同机制旨在打破各防御节点的孤立状态，形成覆盖全网的立体防御体系，具体如下：（1）防火墙作为网络层的第一道屏障，通过制定访问控制策略过滤异常流量，可与终端防护系统共享病毒特征信息，在病毒通过网络传播的初期进行拦截。当终端检测到病毒活动时，可实时向防火墙反馈病毒的网络行为特征，促使防火墙动态更新规则，阻断同类病毒的进一步扩散。（2）入侵检测系统通过对网络流量的深度分析，识别病毒传播过程中的异常行为模式，其检测结果可与终端防护系统形成联动。当入侵检测系统发现可疑流量时，可向对应的终端发送预警信息，触发终端的深度扫描与隔离操作；终端则将病毒的详细特征与行为日志反馈给入侵检测系统，帮助其优化检测模型，提升对隐蔽性病毒的识别能力。（3）协同机制的核心在于建立统一的安全管理平台，实现终端与网络层防护设备的数据互通与策略协同。该平台可集中收集各节点的病毒检测数据，通过关联分析识别病毒的传播规律与攻击路径，自动生成协同防御策略并下发至终端与网络设备[4]。

结束语：计算机网络工程安全与病毒防护是一项复杂的系统工程，需从技术、管理等多维度综合施策。本文通过梳理安全基础、病毒特性，构建防护体系与探讨防护技术，明确了各环节的关键要点。随着网络技术的演进，新的安全威胁将不断出现，需持续优化防护技术与策略，加强跨领域协同，提升安全防护的动态适应性。只有不断创新与完善防护体系，才能为计算机网络的健康发展提供坚实保障。

参考文献

[1]张美琪.计算机网络工程安全与病毒防护[J].数码设计(下),2020,9(10):33-34.

[2]王涛.计算机网络工程安全与病毒防护[J].数码设计(上),2020,9(3):32-33.

[3]董子阳.计算机网络工程安全与病毒防护[J].文渊(高中版),2020(3):839-840.

[4]王斌,梁建霞.计算机网络工程安全与病毒防护分析[J].中国新通信,2020,22(14):165-166.