 DOI: https://doi.org/10.12349/iser.v6i5.5704

The Application of Computer Security Technology in Network Security Maintenance

Wenjiang He

Gansu Finance and Trade Vocational College, Lanzhou City, Gansu Province (730000)

Abstract

With the development of computer networks, network security issues have become increasingly prominent. Network threats have caused serious impacts on enterprise secrets, personal privacy, and national security. Computer network security technology has been constantly innovating and has evolved from the initial cryptography-based methods to the current comprehensive security system that combines data encryption, intrusion detection, firewalls, and other technologies. In the digital age, people are paying more and more attention to network security. The continuous growth of network security and threats has promoted the development of network security technology, which can meet the needs of network security and ensure the safety and development of the digital society. Therefore, this paper studies the application of computer network security technology and proposes feasible network security maintenance solutions.

Keywords

Computer security technology; Network security; Security maintenance; Computer technology

计算机安全技术在网络安全维护中的应用

何文江

甘肃财贸职业学院，中国 · 甘肃 兰州 730000

摘　要

在计算机网络发展中，网络安全问题也越来越突出，网络威胁对企业机密、个人隐私和国家安全造成了严重的影响。计算机网络安全技术在不断的创新，已经从最开始的基于密码学方法发展到目前的数据加密、入侵检测、防火墙等多技术结合的综合安全体系。在数字化时代下，人们越来越重视网络安全，不断增长的网络安全与威胁促进了网络安全技术的发展，能够满足网络安全需求，保证数字化社会的安全性与发展。以此，本文就对计算机网络安全技术的应用进行研究，提出可行的网络安全维护方案。

关键词

计算机安全技术；网络安全；安全维护；电脑技术

1 引言

计算机安全技术能够降低网络数据威胁、侵害的发生几率，使网络可用性得到提高，避免数据泄露。将计算机安全技术应用到网络安全维护中，能够提高网络安全性。目前，计算机安全技术被广泛应用到政府机构和企业中，还能够保护个人的隐私，为现代数字化发展的重点 [1]。

2 计算机安全技术和网络安全维护

2.1 网络安全维护

计算机网络安全维护指的是将不同的技术手段应用到计算机用户或者运维管理系统中，保证网络的稳定性与安全性。一般，计算机网络安全维护技术包括入侵检测系统、防火墙、安全信息、入侵防御系统等。网络安全维护主要目的为创建多维度安全防护体系，避免网络网威胁。但是，传统静态防护方法无法抵御网络威胁。所以，要求使用动态化、智能化的防护技术。

2.2 计算机网络安全的要求

（1）机密性。保证信息未经授权获取访问者，利用身份验证、数据加密等技术在用户通过身份验证或者授权才能够访问敏感信息。

（2）可用性。保证网络与服务的可用性，不会受到恶意攻击或者中断。利用负载均衡与冗余技术，即便是系统中存在大规模流量攻击与硬件故障，网络还能够正常服务。

（3）完整性。在传输过程中的信息不会被修改和篡改，提高数据可用性。

（4）身份验证。在系统与信息访问中，只能够被合法用户访问，通过授权确定合法用户。身份验证包括双因素身

【作者简介】何文江（1968–），男，中国江西南康人，本科，从事计算机技术应用研究。

份验证、用户名与密码等，确定用户身份。在系统内部权限中，保证用户访问合理范围中的资源，避免数据泄露 [2]。

3 网络安全维护的方案设计

3.1 网络安全维护模型的架构设计

计算机网络安全技术为个人信息与各类组织传递信息的平台，在网络安全维护中要融入先进的安全技术，解决复杂的攻击问题。设计基于计算机安全技术的网络维护模型。基础设施层的主要功能为资源的动态调度与虚拟化，使用容器化技术对计算资源进行弹性伸缩；安全分析层和规则引擎与机器学习算法结合，能够全面检测网络威胁；数据处理层利用流式计算框架与分布式存储技术，对海量安全日志进行分析；应用接口层为网络安全维护提供了可视化与统一的安全策略。利用微服务架构实现各层级的松耦合通信，提高系统的容错性。以主从式集群部署方案设计模型，根据负载均衡保证系统的可用性。

使用多层级联动防护策略，以安全编排与自动化响应技术实现网络安全防护。在网络安全防护中，部署可编程数据平面，过滤异常流量，灵活调度流量，以自定义流标规则实现访问控制。以 eBPE 技术对计算机网络安全行为进行监控，满足异常行为检测。另外，还设计了基于 Grafana 的全栈监控，以自定义告警规则自动检测故障，并且对故障进行快速响应。在数据处理过程中，通过数据的收集、分析、清晰和存储方式，以多级流水线的方式处理数据。以分布式日志采集器对安全设备告警、网络流量等异构数据收集，通过 Apache Beam 对数据进行清晰和处理，自定义数据转换算法同意提取字段，创建事件关联图谱，对攻击链路进行识别 [3]。

3.2 计算机网络安全维护方案

3.2.1 Agent 系统的应用

Agent 系统功能为智能化、自主性的软件，在计算机网络安全维护过程中应用的主要功能为执行任务、感知环境，还能够实现系统之间的交互。Agent 能够以不断变化的动态环境调整自身行为。利用高效、灵活性的管理模式，以主动响应、协同防御、自主监控等方法对计算机网络进行安全维护 [4]。聚集不同的网络节点自主控制网络监控行为，设计网络监控不同的方案。针对 Agent 运行中的异常情况及时报警，比如病毒攻击等。在出现网络攻击时更新防火墙的规格，从而隔离病毒，避免对网络运行造成影响，图 1 为 Agent 的运行模式。

3.2.2 威胁检测模型的设计

机器学习联合深度学习的计算机网络安全威胁检测模型为网络安全维护的重点，利用智能算法深度分析网络后，对潜在的威胁进行识别，然后生成网络安全策略。通过此模块和异常行为分析、安全策略生成等功能结合，构成完整的计算机网络安全威胁检测与维护体系。

在计算机网络安全检测中，通过异常行为分析能够学习海量的网络数据，识别偏离原本基线的异常行为。以无监督学习算法发现网络中潜在的异常模式，并通过所标注的威胁样本学习特征，使检测效率得到提高。通过深度学习中的长短时记忆网络 LSTM 与循环神经网络 RNN 对时间序列数据进行处理，实现网络流量时序特征的分析，对复杂攻击行为识别。在响应机制中反馈模型所输出的异常行为，利用预设相应策略抑制实时的威胁，比如系统告警、封锁恶意 IP 地址等。

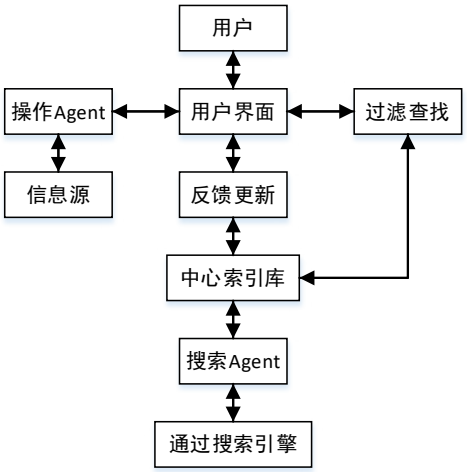

图 1 Agent 的运行模式

动态调整策略能够提高威胁检测运行的效率，通过强化学习算法在仿真环境中进行学习与试探，使用强化学习算法执行策略最优解。和实时反馈及直接和，对策略的执行效果监测，保证防御措施的有效性。

在威胁检测模型中，安全策略生成与更新能够对自动生成策略检测，结合历史攻击与威胁情报库中的数据设计动态化防护对策。在出现网络安全事件的时候，以应急响应机制迅速处理。

利用用户界面与可视化模块创建用户和模型交互的桥梁，以优化界面为用户展现系统的威胁检测结果和运行状态。包括威胁检测日志、网络流量图等，用户及时掌握系统的动态运行情况。将潜在的威胁以电子邮件、弹窗或者短信的方法发送给用户，从而直观掌握安全状态，利用多维数据分析工具对潜在威胁分析，优化系统运行。

3.2.3 虚拟桌面云架构

虚拟桌面云系统架能够使存储资源、计算资源、网络资源构成独立虚拟环境，利用虚拟化技术集中部署桌面操作系统，并且对系统内容进行访问和管理，构成虚拟桌面云架构。用户以终端设备随时的访问虚拟桌面，提高了工作效率。

本文以正则极限学习机 RELM 联合布谷鸟搜索算法 MCS 对网络安全预测的方法进行改进，提高网络安全态势预测的效率和精度，满足多维时间序列的分析价值。此模型的风险评估、网络安全监测与事件响应效果良好，还能够满足复杂网络环境的需求。虚拟桌面云安全防护结构包括业务

层、虚拟防火墙和终端，以输入输出网络数据对网络安全态势进行预测，通过 ACL 安全策略保护云系统的虚拟桌面 [5]。

3.2.4 用户行为分析与预测

用户根据网络行为分析功能对网络流量分析，和各层协议结合实时展现流量情况。另外，此行为分析作为网络安全维护的主要功能模块，能够收集计算机网络基础流量信息，并且对信息进行分析存储。以当前行为创建行为模型，通过收集信息流、行为预测、特征值提取与危险预警等功能，对数据流数据检测和预测，从而制定计算机网络安全维护措施：

（1）行为序列。对用户当前行为进行分析，根据行为相似性对用户进行分类，将现有行为输出后对用户行为序列更新。

（2）行为模式。根据读取操作对用户行为序列分析，如果序列中的数据出现次数比较多，要对其开展序列分析处理，总结当前行为模式。

在分析用户行为后预测使用行为，使管理人员对用户下一步的行为进行预测，从而制定网络安全维护策略。对多用户行为模式进行挖掘，从而生成行为带权有向图。收集不同行为的关系，不需要人工，只需要结合具体需求就能够将预测精度发送到系统中。在得到预测模型后，结合模型与系统开展预测，考虑不同行为的可能性。将带权有向图权值的作用发挥出来。此方法的自适应性良好且灵活，利用预测行为标准和网络用户行为进行对比，提高权值准确性。实时调整网络使用行为权值，提高安全预警系统的精准性。

3.3 虚拟化安全加固

在计算机网络安全维护中，通过虚拟化安全加固的方法进行访问控制，对虚拟机资源的通信和访问进行限制，降低网络横向攻击的潜在风险。根据细粒度访问控制策略与网络隔离、资源配额等规则，设置网络规则集权限，从而访问合法资源。以硬件设备辅助虚拟技术的运行，对访问工作实时监控，比如 AMD-V 等技术。其次，根据虚拟机管理软件监控虚拟机的行为，对异常活动实时监测。假如虚拟机在运行的时候遭到威胁，要及时隔离避免危害。利用网络安全组与防火墙提高网络安全性，避免组件和虚拟机出现漏洞。及时修补漏洞，提高系统的整体抗攻击能力。

综合以上方法能够使虚拟机环境安全性得到提高，使计算机网络在运行过程中抵御潜在安全威胁 [6]。

3.4 虚拟专用网联合安全审计

在计算机网络维护中使用虚拟专用网 VPN 和安全审计技术创建网络安全隧道，对计算机网络进行安全监控，使网络环境安全性得到提高。虚拟专用网的核心就是利用加密通道保护数据传输安全，避免数据被篡改或者截获。此技术一般应用在内部通信组织与企业中，比如某企业利用企业级 VPN 的分支机构实现远程访问权限，使企业员工和企业内部网络的连接更加安全，对敏感企业资源进行访问。此方法能够保证企业远程办公更加的安全，提高企业机密信息处理过程中的效率。

另外，通过安全审计技术详细记录网络活动，深入了解网络安全事件。比如，单位要想实施全面安全审计系统，监控所有用户行为、网络流量和日志，可以对潜在非法问题与安全风险进行识别分析。通过此审计日志，为网络安全专家提供分析基础数据。

综合使用安全审计技术和虚拟专用网，不仅能够对网络安全管理进行优化，还能够增强潜在安全事件响应能力。利用 VPN 安全通信通道，提高了组织安全防护效果，维护网络环境安全性。

4 计算机网络安全维护方案的实验检测

通过 MCS-RELM 网络模型创建计算机网络安全测试环境，使用桌面链路和 Gbps 级别骨干链路配置服务器作为主机。以 VC++ 实现计算机安全保护，在防火墙系统中部署。以黑客数据与技术攻击所设计的计算机网络安全维护系统。通过测试结果表示，本文所设计的网络安全维护方案能够将被动网络防御转变为被动防御，缩短了预测时间，系统的防护能力得到增强。以不同安全模型进行对比，得到实验平均值。在对比指标中，RMSE 为均方根相对误差，MAPE 为平均误差。

5 结语

在现代信息技术环境不断发展中，网络维护中的网络安全技术应用具有重要意义。利用有效的入侵检测、威胁检测模型、用户行为分析等技术，提高了网络整体安全水平。此策略能够解决各种网络威胁，保证用户安全与数据完整性。在网络安全威胁发展下，要持续优化相关的技术，从而提高网络安全性，持久保证信息系统的应用效果。

参考文献

[1] 郭文博. 云计算技术在计算机安全存储中的应用[J]. 电声技术,2022,46(1):29-31.

[2] 肖莉莉. 计算机网络安全技术在网络安全维护中的应用[J]. 数字技术与应用,2022,40(6):222-224.

[3] 马小翠. 数据加密技术在计算机网络安全中的应用探讨[J]. 产业与科技论坛,2021,20(18):42-43.

[4] 李康. 大数据在通信网络安全防范中的应用探究[J]. 科技创新导报,2020,17(32):107-109.

[5] 王峥,崔冉. 基于多源数据挖掘的网络安全态势评估系统[J]. 吉林大学学报（信息科学版）,2025,43(1):143-149.

[6] 刘延华,方文昱,郭文忠,等. 基于联邦增量学习的SDN环境下DDoS攻击检测模型[J]. 计算机学报,2024,47(12):2852-2866.

[7] 赵鹏. 人工智能和大数据技术在计算机网络安全防御中的运用[J]. 通讯世界,2024,31(9):46-48.