

# 计算机网络安全虚拟化技术发展思考

## ——评《计算机网络安全及其虚拟化技术研究》

数字化时代,计算机网络已成为现代社会运转不可或缺的基础设施,其安全性直接关系到数据保护、业务连续性和国家安全。随着云计算、大数据、人工智能等技术的迅猛发展,计算机网络安全面临着前所未有的挑战,而虚拟化技术作为提升网络安全性和灵活性的重要手段,正逐步成为研究和应用的热点。

网络安全是计算机技术可持续发展的重要保障。《计算机网络安全及其虚拟化技术研究》一书共分为8章,主要探讨计算机网络安全及其虚拟化技术。第1章主要介绍了计算机网络的认知、计算机网络安全及其体系结构、计算机信息安全及管理。第2章主要分享了密码学与密码技术、身份认证与访问控制、数据库与数据安全技术。第3章主要阐述了计算机网络空间安全概念、计算机网络舆情的传播与监测、计算机网络空间安全治理。第4章主要讨论了计算机网络系统安全防护、计算机局域网与防火墙安全防护、计算机网络安全分层评价防护体系、移动互联网时代网络安全的防范。第5章讲解了人工智能概述、人工智能安全及发展、人工智能时代了计算机网络安全防护。第6章主要探究了云计算的基础架构与部署模式、云存储与数据安全需求、云计算数据安全的发展。第7章主要讲述了对虚拟化技术的认知与实现、内存虚拟化与存储虚拟化、虚拟专用网技术种类。第8章主要分析了计算机虚拟化技术对资源的控制、计算机虚拟仿真实验平台的设计与实现、计算机虚拟化技术的应用等。

作者指出,计算机网络面临着诸如硬件配置不当、木马与病毒入侵、非法授权访问等的威胁和挑战,网络安全具有重要性和复杂性。虚拟化技术在计算机网络安全中的应用具有提高资源利用率、降低成本等很多优势,也带来了传统安全风险延伸及新技术引入的安全挑战,需要采取相应的安全措施。为此,从技术层面可从边界防御架构向内生安全防御架构转变的策略,以应对虚拟化技术带来的安全风险。作者强调,为保障虚拟化环境中的信息安全,加强身份认证和通信加密具有重要的作用,通过身份认证可确保网络实体的合法性,而通信加密则防止通信链路被窃听和篡改。

笔者认为,虚拟化技术通过将物理资源抽象化,实现资源的灵活分配和管理,为计算机网络安全提供新的解决方案。在网络安全领域,虚拟化技术的应用主要体现在以下几个方面。①隔离与防护。虚拟化技术能够创建独立的虚拟环境,将不同应用或服务隔离运行,有效防止恶意软件在网络中的传播和扩散。如通过虚拟化技术构建沙箱环境,能实现对未知软件的隔离测试,减少其对系统安全的威胁。②动态资源调度。虚拟化技术允许根据实际需求动态调整资源分配,提高系统应对网络攻击的能力。在网络攻击发生时,系统可迅速调整资源分配,隔离受攻击部分,保障整体系统的稳定运行。③安全服务虚拟化。随着虚拟化技术的发展,越来越多的安全服务被虚拟化,如防火墙、入侵检测系统等。这些虚拟化安全服务可灵活部署在网络的各个节点,提高安全防护的效率和灵活性。

尽管虚拟化技术在计算机网络安全中展现出巨大的潜力,但其发展也面临着性能损耗、安全隔离性和管理复杂性等挑战。面对这些挑战,笔者认为,计算机网络安全虚拟化技术的发展将呈现以下趋势。①性能优化,随着硬件技术的不断进步和虚拟化技术的持续优化,虚拟化环境的性能损耗将逐渐降低,如通过采用更高效的虚拟化引擎和更先进的资源调度算法,提高虚拟化环境的整体性能。②安全隔离性增强,为提升虚拟化环境的安全隔离性,研究者将不断探索新的隔离技术和机制。如通过采用更严格的访问控制和隔离策略,以及利用硬件级别的安全隔离技术,有效防止跨虚拟机攻击。③智能化管理,随着人工智能技术的不断发展,智能化管理将成为虚拟化技术发展的重要方向。通过引入机器学习、深度学习等数据分析技术,实现对虚拟化环境的智能监控和管理,提高系统应对网络攻击的能力和效率。

总之,计算机网络安全虚拟化技术作为提升系统安全性、灵活性和资源利用率的重要手段,面对当前存在的挑战和问题,需要不断探索新的技术和方法,推动虚拟化技术的持续优化和发展。同时,加强标准化与规范化建设,提高虚拟化技术的互操作性和兼容性,计算机网络安全虚拟化技术将为构建更加安全、高效、智能的网络环境贡献力量。



书名:计算机网络安全及其虚拟化技术研究

作者:李春平

出版社:中国商务出版社

ISBN:9787510345821

出版时间:2023年1月

定价:65元

(刘慕博/陕西理工大学特莱恩工学院)