第 1 卷◆第 4 期◆版本 1.0◆2023 年
文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

民航空管流量系统虚拟化技术安全问题研究

商亚雯
华北空管局
DOI:10.12238/acair.v1i4.6797

[摘　要] 民航空中交通管制的流量系统是保障民航运行安全、高效的关键环节,随着空中交通流量的持续增长,面临着巨大的压力和挑战。为了提高运行效率和服务质量,虚拟化技术被广泛引入和应用于空中交通管制的流量系统中,虚拟化技术具有提高资源利用率、降低成本、增强灵活性和可扩展性等优势。然而,虚拟化技术的引入和应用也给空中交通管制的流量系统带来了新的安全问题和风险,其中最具代表性和危害性的安全威胁之一就是虚拟化逃逸,即指攻击者利用虚拟化层的漏洞或缺陷,突破虚拟机或容器的限制,实现与宿主机操作系统的交互的攻击手段。一旦发生虚拟化逃逸,攻击者就可以感染宿主机或其他虚拟机,窃取或破坏敏感数据,干扰或瘫痪空中交通管制的流量系统的正常运行,造成严重的后果。因此,本文旨在探讨虚拟化技术在民航空中交通管制的流量系统中的应用和安全问题,以及如何防范和应对虚拟化逃逸等安全威胁。
[关键词] 流量系统；虚拟化漏洞；安全威胁
中图分类号：TK313　文献标识码：A

Research on network security of air traffic control system virtualization technology in civil aviation

Yawen Shang
North China Air Traffic Control Bureau

[Abstract] The air traffic control system in civil aviation is a key link to ensure the safe and efficient operation of civil aviation. With the continuous growth of air traffic, it faces tremendous pressure and challenges. In order to improve operational efficiency and service quality, virtualization technology has been widely introduced and applied to the air traffic control system. Virtualization technology has the advantages of improving resource utilization, reducing costs, enhancing flexibility and scalability. However, the introduction and application of virtualization technology also brings new security issues and risks to the air traffic control system. One of the most representative and harmful security threats is virtualization escape, which refers to the attack method in which attackers exploit vulnerabilities or defects in the virtualization layer, break through the restrictions of virtual machines or containers, and interact with the host operating system. Once a virtualization escape occurs, the attacker can infect the host or other virtual machines, steal or destroy sensitive data, interfere with or paralyze the normal operation of the air traffic control system, causing serious consequences. Therefore, this article aims to explore the application and security issues of virtualization technology in the air traffic control system of civil aviation, and how to prevent and deal with security threats such as virtualization escape.
[Key words] Traffic System; Virtualization Vulnerability; Security Threat

本文旨在探讨虚拟化技术在民航空中交通管制的流量系统中的应用和安全问题，以及如何防范和应对虚拟化逃逸等安全威胁。本文的主要内容包括以下几个方面：首先，介绍虚拟化技术在民航空中交通管制的流量系统中的应用场景和价值，以及应用效果和存在的问题；其次，介绍虚拟化逃逸的概念、原理和特征，以及对民航空中交通管制的流量系统的威胁和影响；再次，介绍防范和应对虚拟化逃逸的基本原则和目标，以及具体措施和方法；最后，总结本文的主要观点和结论，展望本文的研究前景和意义。

1 虚拟化技术在民航空中交通管制流量系统中的应用

虚拟化技术是指通过软件的方式，将物理资源（如服务器、

网络、存储等)抽象、隔离和转换,从而创建出多个逻辑资源,实现对物理资源的动态分配和管理的技术。虚拟化技术具有提高资源利用率[①]、降低成本、增强灵活性和可扩展性等优势,为空中交通管制的流量系统提供了新的可能性和机遇。

虚拟化技术,通过软件方式将物理资源抽象、隔离和转换,为空中交通管制的流量系统提供了新的可能性和机遇。其应用场景和价值主要体现在以下几个方面：

虚拟机：在一台物理机上运行的多个独立的操作系统和应用程序的环境,可以实现对物理机的高效利用,提高流量系统的计算能力和可靠性。例如,流量系统可以使用虚拟机来部署多个不同的流量管理应用,实现应用的快速部署、迁移和恢复。

虚拟网络：在物理网络的基础上,通过软件的方式,创建出多个逻辑上的网络,实现对物理网络的动态配置和管理。例如,流量系统可以使用虚拟网络来构建多个不同的网络域,实现网络域之间的隔离和通信。

虚拟存储：在物理存储的基础上,通过软件的方式,创建出多个逻辑上的存储,实现对物理存储的动态分配和管理。例如,流量系统可以使用虚拟存储来存储和备份大量的流量数据,实现数据的快速访问、迁移和恢复。

虚拟化技术在民航空中交通管制的流量系统中的应用效果和存在的问题主要体现在以下几个方面：

提高运行效率：虚拟化技术可以实现对流量系统的资源的高效利用和优化,提高运行效率。例如,虚拟化技术可以实现对流量系统的计算、网络、存储等资源的动态分配和调整,根据空中交通流量的变化,合理分配和利用资源。

降低航班延误：虚拟化技术可以实现对流量系统的资源的灵活配置和扩展,降低资源的不足和故障的风险,降低航班延误的概率和程度。例如,虚拟化技术可以实现对流量系统的资源的动态扩展和增强,根据空中交通流量的峰值和突发情况,及时增加和提升资源的容量和性能。

缓解空域压力：虚拟化技术可以实现对流量系统的应用和数据的高效处理和分析[②],缓解空域压力。例如,虚拟化技术可以实现对流量系统的流量数据的高效处理和分析,根据流量数据的特征和规律,制定合理的流量预测、流量规划、流量控制等策略,优化空中交通流量的分布和安排。

2 虚拟化逃逸及其对民航空中交通管制的流量系统的威胁

虚拟化逃逸是一种高级的安全威胁,攻击者利用虚拟化层的漏洞或缺陷,突破虚拟机或容器的限制,实现与宿主机操作系统的交互。这对民航空中交通管制的流量系统中的虚拟化技术应用和安全构成了严重的挑战。

攻击对象是虚拟化层,例如虚拟机监控器(VMM)或虚拟化层的软件或硬件组件[①]。攻击方式是利用虚拟化层的漏洞或缺陷,执行恶意的代码或指令,实现从虚拟机或容器到宿主机操作系统的跳转和交互。

这种攻击的原理是利用虚拟化层的漏洞或缺陷,绕过虚拟化层的安全机制,实现对虚拟化层的控制和修改,从而实现对宿主机操作系统的访问和控制。虚拟化层的安全机制包括隔离机制、监控机制和保护机制。它特征包括隐蔽性、复杂性和危害性。攻击者通常通过虚拟机或容器的正常的请求和操作,来隐藏和传播恶意的代码或指令。攻击者需要具备高级的技术和知识,才能成功地实施虚拟化逃逸的攻击。一旦攻击者成功地实现了对宿主机操作系统的访问和控制,就可以对宿主机操作系统和其他虚拟机或容器进行各种恶意的操作,造成严重的安全后果。

虚拟化逃逸对民航空中交通管制的流量系统的威胁和影响主要体现在以下两个方面：破坏虚拟化的隔离性和安全性,以及感染宿主机或其他虚拟机。虚拟化逃逸的攻击者通过突破虚拟化层的隔离和监控机制,实现对宿主机操作系统的访问和控制,从而破坏了虚拟化技术的基本特性和优势。此外,攻击者通过控制和修改虚拟化层的代码和数据,实现对宿主机操作系统和其他虚拟机或容器的感染和攻击,从而扩大了虚拟化逃逸的攻击范围和影响程度。这可能导致空中交通管制的流量系统的功能和性能的严重下降和损失[②],甚至导致空中交通管制的流量系统的完全瘫痪和崩溃。因此,对虚拟化逃逸的防范和应对是保障民航空中交通管制的流量系统安全的重要任务。

3 防范和应对虚拟化逃逸的对策和建议

虚拟化逃逸是一种对虚拟化技术的高级安全威胁,对民航空中交通管制的流量系统构成了严重挑战。防范和应对虚拟化逃逸的攻击需要采取多方面的对策,提高虚拟化安全的水平和能力。

首先,遵循最小权限原则,为每个虚拟机或容器分配最小的必要资源和权限,限制其访问和操作范围,降低虚拟化逃逸的攻击可能性和危害性。例如,空中交通管制的流量系统可以根据虚拟机或容器的功能和需求,为其分配合适的计算、网络、存储等资源[③],提高资源的使用率和性能。同时,也可以根据虚拟机或容器的安全等级和敏感性,为其分配合适的权限和角色,提高权限的合理性和安全性。

其次,实施多层防御策略,在虚拟化层、宿主机操作系统、虚拟机或容器等不同层次上,采用不同的技术和方法,构建多层防御体系,防止虚拟化逃逸的攻击的发生和扩散,提高虚拟化安全的强度和深度。例如,空中交通管制的流量系统可以在虚拟化层上,使用虚拟化层的安全机制,如隔离、监控、保护等,对虚拟化层的代码和数据进行检查和验证,提高虚拟化层的稳定性和安全性。同时,也可以在宿主机操作系统上,使用宿主机操作系统的安全机制,如防火墙、杀毒、加密等,对宿主机操作系统的资源和服务进行保护和控制,提高宿主机操作系统的可靠性和安全性。再者,也可以在虚拟机或容器上,使用虚拟机或容器的安全机制,如沙盒、审计、隔离等,对虚拟机或容器的运行和行为进行监视和管理,提高虚拟机或容器的合法性和安全性。

此外,提高安全意识和能力也是非常重要的。空中交通管制

的流量系统的管理者和使用者可以通过学习和培训，提高对虚拟化技术和虚拟化安全的知识和技能，增强对虚拟化逃逸的攻击的警惕和防范，提高对虚拟化逃逸的攻击的发现和应对的能力④。同时，也可以通过规范和监督，提高对虚拟化技术和虚拟化安全的规范和负责，遵守和执行虚拟化安全的规则和标准，提高虚拟化安全的质量和效果。

最后，选择可靠的虚拟化平台和产品，以及及时更新和修复虚拟化层的漏洞，也是防范和应对虚拟化逃逸的重要措施。空中交通管制的流量系统可以选择经过严格测试和验证，具有良好声誉和评价，符合国际标准和行业规范的虚拟化平台和产品，避免使用未经授权或未经认证的虚拟化平台和产品，防止虚拟化平台和产品的质量和安全问题。同时，也需要及时更新和修复虚拟化层的漏洞，防止虚拟化逃逸的攻击的发生。

4 结语

本文探讨了虚拟化技术在民航空中交通管制的流量系统中的应用和安全问题，以及如何防范和应对虚拟化逃逸等安全威胁。虚拟化技术在民航空中交通管制流量系统中有广泛的应用和重要的价值，可以提高系统的资源利用率、运行效率、网络效率、存储容量、安全性等方面的性能，降低航班延误的概率和程度，缓解空域压力，为民航运行安全、高效、绿色做出贡献。

然而，虚拟化技术也面临着虚拟化逃逸等安全威胁，这是一种针对虚拟化技术的高级的安全威胁，具有隐蔽性、复杂性和危害性，可以破坏虚拟化的隔离性和安全性，感染宿主机或其他虚拟机，窃取或破坏敏感数据，干扰或瘫痪空中交通管制的流量系统的正常运行，造成严重的后果。

防范和应对虚拟化逃逸的攻击需要从多个方面采取相应的对策和建议，提高虚拟化安全的水平和能力，包括遵循最小权限原则，实施多层防御策略，提高安全意识和能力，选择可靠的虚拟化平台和产品，及时更新和修复虚拟化层的漏洞，加强虚拟机的配置和管理，隔离和监控虚拟机的网络和存储，使用安全工具和技术等。

随着民航业的发展和虚拟化技术的进步，虚拟化技术在民航空中交通管制的流量系统中的应用将更加广泛和深入，虚拟化安全将成为民航空中交通管制的流量系统的重要保障，也将为民航安全、高效、绿色运行做出更大的贡献。随着虚拟化技术的复杂性和多样性的增加，虚拟化逃逸等安全威胁也将更加隐蔽和危险，防范和应对虚拟化逃逸的攻击将更加困难和挑战，需要不断地研究和探索新的虚拟化安全的问题和风险。

注释：

①《中国民航报》,胡夕姮:“激活智慧空管系统的“神经末梢””,载《中国民航网》,2022年9月14日。

①“虚拟机逃逸问题分析与防范 - FreeBuf网络安全行业门户”,2020年10月19日。

②《安全内参》:“未来天空的新兴技术：虚拟化”,2022年7月19日。

②“基于功能脆弱性的空中交通相依网络流量分配”,王兴隆，齐雁楠，潘维煌,《航空学报》,2020年。

③《中国民航报》，胡夕姮:“激活智慧空管系统的“神经末梢””,载《中国民航网》,2022年9月14日。

④《国家保密局互联网门户网站》:“虚拟机逃逸安全研究”,2021年5月13日。

[参考文献]

[1]周福臻.激活“神经末梢”打造“堡垒前哨”[J].湖北教育,2023,(21):40,44.

[2]殷梦瑶.VoIP技术在民航空管语音通信系统中的运用[J].通信电源技术,2022,39(7):122-124.

[3]范成龙.基于QEMU的虚拟机逃逸关键技术研究[D].河南:郑州大学,2018.

[4]王兴隆,齐雁楠,潘维煌.基于功能脆弱性的空中交通相依网络流量分配[J].航空学报,2020,41(4):179-187.

[5]李蓓,王智明,李云庆.突触前神经末梢的钙离子通道[J].中国神经科学杂志,2004,20(6):471-475.

[6]范伟.虚拟机逃逸安全研究[J].保密科学技术,2020,(10):9-14.

作者简介：

商亚雯(1996--),女,汉族,河北省石家庄市人,本科,助理工程师,研究方向：民航空管系统通信导航监视的网络安全方向。