民航空管场景下的网络攻击手段与防范策略探析

魏子涵
成都西南民航通信网络有限公司　四川　成都　610000

摘　要：民航空管系统作为确保飞行安全与效率的核心，面临着复杂的网络攻击挑战。本文系统分析了民航空管场景下常见的网络攻击手段，如弱口令攻击、后门入侵、系统漏洞利用、DDoS攻击及GPS欺骗等，这些攻击对空管系统的稳定性和安全性构成严重威胁。同时，本文提出了针对性的防范策略，旨在加强系统安全防护，确保民航空管系统的稳定运行和飞行安全。

关键词：民航空管场景；网络攻击手段；防范策略

引言：民航空管系统是民用航空安全高效运行的重要保障。然而，随着信息技术的广泛应用，其面临的网络攻击风险也显著增加。本文旨在全面分析民航空管场景下的网络攻击手段，包括但不限于弱口令攻击、后门攻击、系统漏洞利用等，同时深入探讨有效的防范策略。通过本研究，期望为空管系统的安全防护提供科学依据和实践指导，以保障航空运输的安全顺畅，维护国家空域资源的有效利用。

1 民航空管系统概述

1.1 民航空管系统的定义与功能

民航空管系统，即民用航空空中交通管理系统，是保障民用航空活动安全、有序、高效进行的关键基础设施。其核心功能涵盖空中交通管理、航班信息管理以及飞行安全监控等多个方面。（1）空中交通管理：负责监控全国乃至全球的航空器运行状态，通过雷达、通信等设备实时掌握航空器的位置、速度、高度等信息，并据此进行指挥与调度，确保飞行航线不冲突，空中交通流畅安全。（2）航班信息管理：整合并分析来自航空公司、机场、气象等多个渠道的信息，提供航班计划、航班动态、延误预警等实时数据，为航班运营提供决策支持，优化飞行资源配置。（3）飞行安全监控：利用先进的监控技术和算法，对飞行过程中的关键参数进行实时监测与分析，如飞机发动机性能、飞行姿态等，及时发现并预警潜在的安全风险，确保飞行全过程的安全。

1.2 民航空管系统的网络架构

民航空管系统的网络架构复杂且高度集成，主要包括整体结构、关键设备与节点以及网络协议与通信方式三部分。（1）整体结构描述：采用分层分布式架构，由中央处理中心、区域管制中心、终端管制中心等多个层级组成，各层级之间通过高速通信网络相连，形成覆盖全国乃至全球的空管网络。（2）关键设备与节点分析：雷达系统、自动相关监视系统（ADS-B）、甚高频（VHF）通信设备等是空管系统的基础设施，负责数据的采集、传输与处理。其中，雷达系统是空中交通管理的重要工具，ADS-B则提供了更加精确、实时的航空器位置信息。（3）网络协议与通信方式：遵循国际民用航空组织（ICAO）制定的航空通信协议，采用卫星通信、光纤通信等多种通信方式，确保数据的实时、准确传输。此外，空管系统还采用了先进的加密技术，保障数据传输过程中的安全性[1]。

1.3 民航空管系统面临的安全挑战

随着航空业的快速发展，民航空管系统面临着日益严峻的安全挑战。（1）用户终端访问量剧增：随着航班量的持续增长，空管系统需要处理的数据量急剧增加，对网络带宽、存储及处理能力提出了更高要求，增加了系统瘫痪的风险。（2）系统复杂性与兼容性要求：空管系统涉及众多异构设备、软件及通信协议，其复杂性与相互之间的兼容性成为安全管理的难点，增加了系统被攻击或出现故障的可能性。（3）外部网络威胁与内部安全漏洞：网络攻击、病毒入侵等外部威胁以及内部人员误操作或蓄意破坏等内部安全漏洞，都可能对空管系统的稳定运行造成严重影响，进而危及飞行安全。

2 民航空管场景下的网络攻击手段

2.1 弱口令攻击

（1）弱口令的定义与危害。弱口令是指用户设置的密码强度不够，容易被猜测或破解。这些密码可能包括常见的数字、字母组合，或者与个人信息相关，如生日、电话号码等。弱口令的存在给攻击者提供了可乘之机，一旦攻击者成功破解密码，就可以轻松进入系统，获取敏感信息或进行破坏。（2）常见的弱口令攻击方式。爆破口令：攻击者使用字典文件或暴力破解工具，尝试各种可能的密码组合，直到找到正确的密码；利用

Python脚本：编写Python脚本，通过自动化工具快速尝试大量密码，提高破解效率。（3）攻击案例分析。在某次民航空管系统中，攻击者利用爆破口令的方式成功破解了一名员工的登录密码。通过该员工的账户，攻击者进入了系统内部，获取了关键设备的控制权限，并试图进行恶意操作。幸好系统及时发现了异常登录行为，并采取了应急措施，才避免了更严重的后果。

2.2 后门攻击

（1）后门攻击的原理与特点。后门攻击是指攻击者在系统中预留一个“后门”，以便在未来随时进入系统进行恶意操作。这种攻击方式通常隐蔽性较强，难以被检测。（2）常见的后门攻击手段。利用服务器后门：在服务器上安装恶意软件，为攻击者提供远程访问的通道；木马程序：通过伪装成合法的软件或程序，诱导用户下载并运行，从而在系统中植入后门[2]。（3）攻击案例分析。在某次民航空管系统遭受的攻击中，攻击者通过木马程序成功在系统中植入了后门。利用这个后门，攻击者可以随时进入系统查看和修改数据，甚至控制关键设备的运行。系统管理员在发现异常后，立即进行了排查和修复，但这次攻击已经给系统安全带来了极大的威胁。

2.3 系统漏洞攻击

（1）系统漏洞的分类与产生原因。系统漏洞是指系统中存在的缺陷或弱点，可能被攻击者利用来发起攻击。这些漏洞可能源于编程错误、设计缺陷、配置不当等原因。（2）常见的系统漏洞攻击方式。SQL注入：通过向数据库查询语句中注入恶意代码，绕过身份验证或权限控制；跨站脚本攻击（XSS）：攻击者将恶意脚本嵌入到网页中，当用户浏览该网页时，恶意脚本就会执行。（3）攻击案例分析。在某次民航空管系统中，攻击者利用SQL注入漏洞成功获取了数据库的访问权限。通过操作数据库，攻击者可以查询、修改和删除系统中的数据，导致关键信息泄露或系统瘫痪。这次攻击给民航空管系统的运行带来了极大的风险。

2.4 分布式拒绝服务攻击（DDoS）

（1）DDoS攻击的定义与特点。DDoS攻击是指攻击者利用大量计算机或网络设备同时向目标系统发送大量虚假流量，导致系统资源耗尽，无法为正常用户提供服务。（2）DDoS攻击对民航空管系统的影响。DDoS攻击可能导致民航空管系统瘫痪，无法正常处理飞行计划、监控飞行状态等重要任务。这将严重威胁飞行安全，可能导致严重后果。（3）攻击案例分析。在某次DDoS攻击事件中，攻击者利用大量僵尸网络向民航空管系统发送了大量虚假流量。系统因无法承受如此大的负载而崩溃，导致关键服务中断。经过紧急处理和恢复工作，系统才逐渐恢复正常运行。

2.5 GPS欺骗攻击

（1）GPS欺骗攻击的原理与方法。GPS欺骗攻击是指攻击者通过发送伪造的GPS信号来干扰或误导接收器的正常工作。这种攻击可以导致接收器无法接收到正确的卫星信号，从而无法提供准确的定位和导航信息。（2）GPS欺骗攻击对飞行安全的影响。GPS欺骗攻击对飞行安全构成了极大的威胁。在飞行过程中，精确的导航信息是确保飞机按预定航线安全飞行的基础。如果GPS信号被篡改或伪造，将导致飞机接收到错误的位置、速度和时间信息，进而可能引发一系列严重的安全问题[3]。（3）攻击案例与趋势分析。近年来，已经发生了多起GPS欺骗攻击的案例。例如，在某次实验中，攻击者成功利用自制的GPS欺骗设备干扰了无人机的导航系统，导致其偏离了预定航线。这些案例表明，GPS欺骗攻击已经成为一种现实存在的网络威胁，必须引起高度重视。

3 民航空管场景下的网络防范策略

3.1 加强口令管理

（1）提高密码复杂度要求。为确保口令的安全性，应制定严格的密码复杂度政策。这包括要求密码包含大小写字母、数字和特殊字符的混合，以及设置最小长度限制。通过提高密码的复杂度，可以显著增加暴力破解的难度，从而保护系统免受非法入侵。（2）定期更换密码与强制密码策略。定期更换密码是保持口令安全性的有效手段。应制定并执行定期更换密码的政策，如每三个月或六个月更换一次。同时，为避免用户重复使用旧密码或简单修改密码以规避更换要求，应实施强制密码策略，如要求新密码与旧密码在字符序列、长度和复杂度上保持显著差异。（3）利用多因素身份认证技术。多因素身份认证技术通过结合密码、生物特征识别、手机验证码等多种认证方式，为系统提供了更为可靠的身份验证机制。在民航空管系统中，应广泛应用多因素身份认证技术，以提高系统的安全性和可信度。

3.2 系统加固与漏洞修复

（1）定期进行系统更新与补丁安装。系统更新和补丁安装是修复已知漏洞、提升系统安全性的重要手段。应定期关注并及时安装操作系统、应用程序以及安全软件的更新和补丁，以确保系统处于最新的安全状态。（2）加强系统边界防御与入侵检测。系统边界是网络安全防护的重点区域。应加强防火墙、入侵检测系统（IDS）等安全设备的部署和配置，对进出系统的网络

流量进行实时监控和过滤。同时，应定期更新防火墙规则和入侵检测策略，以应对不断变化的网络攻击手段。（3）漏洞扫描与风险评估。定期进行漏洞扫描和风险评估是发现潜在安全威胁、制定针对性防范措施的重要手段。应利用专业的漏洞扫描工具对系统进行全面扫描，及时发现并修复存在的漏洞。同时，结合风险评估结果，制定针对性的安全加固方案，以降低系统被攻击的风险[4]。

3.3 后门防范与监控

（1）扫描与过滤可疑端口。利用端口扫描工具定期对系统上的开放端口进行扫描，及时发现并关闭不必要的端口。同时，应配置防火墙规则，过滤掉来自可疑IP地址的流量，以降低后门攻击的风险。（2）监控与排查可疑进程。利用系统监控工具实时监控系统上的进程和服务，及时发现并排查可疑进程。通过对比正常进程列表和异常进程特征，可以快速定位潜在的后门程序，并采取相应的隔离和清除措施。（3）建立安全审计与事件响应机制。建立完善的安全审计和事件响应机制，记录并分析系统上的所有安全事件和异常行为。通过安全审计日志，可以追溯攻击者的行为轨迹，并为事件响应提供有力支持。同时，应制定详细的应急响应计划，确保在发生安全事件时能够迅速做出反应并恢复系统正常运行。

3.4 DDoS攻击防范

（1）构建流量筛选及净化机制。在网络入口部署流量清洗设备或服务，对进入系统的流量进行筛选和净化。通过识别并过滤掉恶意流量，可以减轻系统的负载压力并保护关键服务不受影响。（2）采用分布式架构设计。通过采用分布式架构设计，将系统分解为多个独立的组件或服务，并确保每个组件都具有冗余和容错能力。这样，即使部分组件受到攻击，整个系统仍然能够保持正常运行。（3）弹性扩展与负载均衡技术。利用弹性扩展和负载均衡技术，根据系统负载情况动态调整资源分配。在面临DDoS攻击时，可以迅速增加系统资源以应对突发的流量高峰，确保关键服务不受影响。通过负载均衡器将流量分散到多个服务器或节点上，避免单点过载，提高系统的整体抗攻击能力。

3.5 GPS欺骗防范

（1）加强GPS信号监控与验证。在系统中部署GPS信号监控设备，实时检测并分析GPS信号的强度、频率和质量等关键参数。通过对比多个GPS接收器的数据，可以识别出异常的GPS信号并触发警报。同时，利用其他导航手段（如惯性导航系统、雷达等）对GPS信号进行交叉验证，确保导航信息的准确性。（2）建立应急响应与处置流程。制定详细的应急响应计划，明确在发生GPS欺骗攻击时的处置流程和责任分工。一旦发生攻击，应立即启动应急响应机制，采取隔离、切断受影响设备等措施，防止攻击扩散。同时，启动备用导航系统或手动飞行模式，确保飞行安全。

结束语

综上所述，民航空管系统作为民用航空的中枢神经，其网络安全防护至关重要。本文不仅深入剖析了多种针对空管系统的网络攻击手段，还提出了一系列切实可行的防范策略。面对日益复杂的网络威胁环境，我们应不断加强技术研发，提升安全防护能力，确保空管系统的稳定运行。未来，还需持续关注网络安全新动态，为空管系统的长期安全发展奠定坚实基础，保障民航事业的持续繁荣与进步。

参考文献

[1]唐杰.浅谈民航空管网络与信息安全管理体系的构建[J].电脑迷,2020,(02):21-22.

[2]吴昊,李上.民航空管场景下的网络攻击手段与防范策略探析[J].电脑知识与技术:学术版,2023,(09):79-80.

[3]胡嘉文.民航空管网络信息安全保障分析[J].科学与财富, 2020,(11):108-109.

[4]王尉舟.基于民航空管的网络与信息安全管理体系的构建[J].中国科技期刊数据库:工业A, 2021,(07):67-68.