IAF SYMPOSIUM ON INTEGRATED APPLICATIONS (B5)
Integrated Applications End-to-End Solutions (2)

Author: Prof. Marek Košuda
Technical University Košice, *(country is not specified)*

Dr. Marian Podmajersky
Technical University Košice, Slovakia

ANYVAULT: LOOKING BEYOND PRIME APPLICATIONS OF PNT DATA

Abstract

The proliferation of Unmanned Aerial Systems (UAS) and Urban Air Mobility (UAM) necessitates a robust security framework to address critical vulnerabilities in low-altitude airspace operations. Current surveillance technologies lack adequate security, exposing operations to spoofing, tampering, and unauthorized access. This proposal introduces "AnyVault," a federated and agnostic security layer designed to secure data throughout its lifecycle, from aggregation to processing.

AnyVault addresses three key needs: secure airborne telemetry, robust authentication and authorization, and efficient asset management. The architecture decouples service functionality and infrastructure, separating core services from access layers. This ensures a secure and resilient ecosystem for UAS/UAM operations. The system comprises peripherals (transmitters, receivers, processors) interacting with the AnyVault service, managed by AnyVault Service Management, which oversees lifecycle functionalities like discovery and monitoring. The AnyVault Cyber Service stack provides microservices for customization, while the AnyVault Core handles authentication, authorization, and assurance. The AnyVault Storage and Computing Infrastructure supports these services, and AnyPNT enhances edge computing for next-generation Network ID and surveillance.

Key security features include silicon-rooted cryptography, stateless encryption, multi-channel redundancy, and a zero-trust model. These measures mitigate vulnerabilities in systems like RemoteID, ensuring data integrity and preventing unauthorized access. End-to-end data security with on-board root-of-trust is achieved through robust cryptographic protocols and tamper-proof hardware.

The proposal aligns with NIS2 compliance, emphasizing asset discovery, vulnerability scanning, and incident response. Efficient asset management is enhanced through secret rotation strategies to counter anti-tampering, anti-spoofing, and anti-replay attacks. The architecture is designed to be agnostic to specific airborne platforms and traffic management systems, ensuring seamless operation across air and ground elements.

Leveraging ESA satellite data, particularly EGNOS and Galileo OS-NMA, enhances positioning, navigation, and timing (PNT) accuracy. Open blueprints and free-to-use firmware promote interoperability and scalability, facilitating widespread adoption and compliance with emerging cybersecurity standards. AnyVault provides a comprehensive security framework, ensuring data integrity, regulatory compliance, and operational safety for the evolving UAS/UAM landscape.