International Civil Aviation Organization

WORKING PAPER

A41-WP/241
EX/108
2/8/22

ASSEMBLY — 41ST SESSION

EXECUTIVE COMMITTEE

Agenda Item 14: Aviation Security — Policy

SECURING AVIATION THROUGH THE ZERO-TRUST APPROACH

(Presented by South Africa)

EXECUTIVE SUMMARY

The aviation industry is sometimes dependant on extended supply chains spanning across varying industries and thus increasing the aviation threat landscape. The adoption of internet protocol (IP) based systems to improve efficiency demands the adoption of proactive approaches necessary to safeguards current and legacy system.

The ICAO Cybersecurity Action Plan outline the need to focus resources and action to achieve systematic approach to managing cybersecurity in aviation; with the objective of developing systems approach that enables aviation to adapt in a timely manner and to withstand new threats.

This working paper seeks to introduce the concept of Zero Trust, that the States and other aviation participants could adopt as one mitigation principle. The incorporation of Zero Trust has the potential to bolster the current cybersecurity protection capabilities through enforcing end to end systems protection. It moves away from traditional perimeter security, through implementing security resources at edge or closer to end user traffic controls facilities and remote sites (supply radar) ground-based navigation aid data.

Action: The Assembly is invited to:

a) recognize the benefit of implementing agile and adaptive Continuous, Adaptive Risk, and Trust Assessment (CARTA) approaches in safeguarding aviation operations;
b) request ICAO through the Cybersecurity Panel to develop technical guidance material to support States in incorporating Zero Trust framework in the information security management systems (ISMS); and
c) urge States to consider incorporating Zero Trust principles in their ISMS.

Strategic Objectives:	This working paper relates to the *Security and Facilitation* Strategic Objective
Financial implications:	No additional budget implications, as this will take place within the budget allocated within ICAO.
References:	*Cybersecurity Action Plan* Doc 8973, *ICAO Aviation Security Manual*

1. INTRODUCTION

1.1 In recent years, the aviation industry has experienced a transformation fuelled by technological adoption and as a result, an increase in the cyber risks that require focus. Through the unpreceded giant leap in terms of technological adoption, which necessitates the continually adoption of Continuous, Adaptive Risk, and Trust Assessment (CARTA) approaches and models.

1.2 The aviation industry has previously been viewed in isolation. However, the interdependency and convergence of Information Technology (IT) / Operational Technology (OT) in aviation ecosystem has introduced various stakeholders who are not governed by aviation compliance mechanisms. This has increased the possible cyber-attack surface and requires that certain traditional concepts to be revised.

1.3 Previously, the management and maintenance of aviation hardware and software could be achieved through secure trusted remote access VPN, which in today's world has led to systems being security compromised experience through such connections.

1.4 Cyber threats such as ransomware, data theft, and phishing attacks have become prevalent in the aviation industry, thus affecting IT (ERP access, collaboration services, e-mail services) and Operational Technology environments (SCADA, PLC's) targeting control areas in and around airports and data centres.

2. DISCUSSION

2.1 The aviation extended supply chain has the potential to introduce cyber threats and thus elevate the need for innovative and new approaches to respond accordingly to these threats. This is due to aviation being dependant on multiple stakeholders that have different systems, applications and technology that need to integrate with one another.

2.2 Key to note is also that enablement of these operations may require remote support from resources based within and outside of a state's borders which further exposes the air transportation value chain to cyber threats.

2.3 Previous, legacy methods of perimeter-based network security which were used to address the security required, have proved to be ineffective. This is evident in the increase in aviation cyber events. Once attackers breach the perimeter, further lateral movement is unhindered.

2.4 Concepts such as Zero Trust have the potential to address next generation and advanced threats that are prevalent today. Allowing for each request for resources, to invoke a process of posture assessment, posture validation and granting of access to resources under considered and effective security controls.

2.5 Zero Trust provides a set of guiding principles for workflow, system design and operations that can be used to improve the security posture for critical and sensitive activities. With the purpose of preventing data breaches and to limit internal lateral movements.

2.6 The Zero Trust approach assumes that no one can be trusted whether inside or outside the organization. This approach seeks to minimize the attack surface based on the following key ideas:

a) the perimeter does not exist. Through eliminating the assumption that people are to be trusted because they have entered inside a company network;

b) ensuring verification of users prior to granting access and verifying device integrity before connecting to the network;

c) eliminate the assumption that users will do the right things. Instead, require verified access rights for each request for service; and

d) rather than tracking bad actors, set up impediments to slow down performance.

2.7 The incorporation of Zero Trust has the potential to bolster the current cybersecurity protection capabilities through enforcing end to end systems protection. It moves away from traditional perimeter security, through implementing security resources at edge or closer to end user traffic controls facilities and remote sites (supply radar) ground-based navigation aid data.

2.8 The implementation of Zero Trust is supported by different underlying technologies that offer protection on various fronts:

a) micro segmentation the earliest concepts of Zero Trust, which is primarily designed to protect against lateral movement to minimize the impact of a breach. Lateral movement to capture information from key assets in the data centre is a central component of several attacks. This approach aims to limit unsanctioned communication between workloads if they have no operative reason to do so, through minimizing breach impact. Unlike typical north-south protection offered by firewalls, micro segmentation looks at east-west security for workloads;

b) Zero Trust network access creates a context-based logical boundary for application access. The goal is to minimize access and abuse by user- and device-context-driven application access. It challenges the assumption that the location of an entity (e.g., inside a network) is to be granted trust automatically;

c) it hides all applications on the network and allows access based on attributes such as user identity, device, geolocation and security posture. Meaning that, users get access to applications they need, but they see nothing else on the network; and

d) remote browser isolation operates on the principle that end users represent the weakest links in any organization and Internet access is one of the largest attack surfaces responsible for breach origination. Therefore, one of the most effective ways to minimize the end point/end user compromise is to isolate web access to eliminate browser exploits and threats such as ransomware, embedded malware and phishing.

3. CONCLUSION

3.1 The Zero Trust principles can be used to ensure that civil aviation is self-strengthening by adopting a “built-in security” approach. Ensuring the security of critical elements and processes “by design” changes the security paradigm from reactive (bolted-on) to proactive and fosters the development of a self-strengthening civil aviation system, therefore enabling it to evolve and enabling improved resilience in a more automated manner, were proven effective.

— END —