International Civil Aviation Organization

Ninth Meeting of the Aeronautical Communication Services Implementation Coordination Group (ACSICG/9)

Video Tele-Conference, 19 - 21 April 2022

Agenda Item 8: Issues on AFS related cyber-safety/security and resilience

AERONAUTICAL FIXED SERVICE (AFS) CYBERSECURITY CONSIDERATIONS FOR INFORMATION OVER CRV

(Presented by United States / FAA)

SUMMARY

This paper presents some security considerations for CRV data exchanges in the light of increased Cyber Threat because of World events.

1. INTRODUCTION

1.1 The 2021 Regional Cybersecurity Webinar[1] presented the work of the International Aviation Trust Framework (IATF) initiative. The IATF is composed of Digital Identity and Network Information Security elements. At the Twenty Fifth Meeting of the Communications Navigation and Surveillance Sub-group (CNS SG/25), WP32 discussed the implications and challenges of these concepts for existing and proposed services in the Asia Pacific Common AeRonautical Virtual Private Network (CRV).

1.2 Although comprehensive in its approach, implementation of the IAFT is still some way in the future. Meanwhile, world events have increased the concern about Cyber Security and the introduction of new functionality is on the horizon. This paper presents some interim security considerations.

2. DISCUSSION

Digital Identity

2.1 The IATF Digital Identity concept uses Public Key Infrastructure (PKI) Digital Certificates to identify the correspondents of an information exchange and potentially secure or encrypt the exchanged data. A Digital Certificate is issued by a trusted authority, using a Public/Private key technique so that the holder can be validated. Technically, the concept is well understood but global implementation for aviation will require policies, trust anchors, trust

[1] Asia/Pacific Regional Cyber Security Webinar: *"Cyber Security Management Framework for CNS/ATM Systems"*, 14 June 2021

bridging, domain naming, managed services, monitoring, auditing, and legal agreements covering terms, liabilities, indemnifications and warranties.

2.2 The CRV was envisioned as a replacement for point-to-point telco between participating ANSPs but its success has attracted other potential users. In the interim before Digital Identity, States must resort to existing methods to identify and manage their networked communications:

- Formalize the communication between parties with technical agreements clearly identifying the information to be exchanged.
- Identify and maintain IP addresses for the exchange and have agreements and procedures prior to changing them.
- Maintain tunnels between communicating parties (e.g. CRV GRE tunnels) that codify a State's formal exchange agreements and implement the agreed IP addresses.
- Use IPsec tunnels if communicating over public networks.
- Implement Access Control Lists (ACLs) on edge and firewall devices such that only the allowed IP/port addresses are permitted.
- Manage the introduction of new network users; non-ANSPs should require sponsorship by the ANSP with which they will communicate.
- Use public networks (e.g. Internet, Cloud) for ANSP data publication and private networks (e.g. CRV) for data receipt and exchange. This limits the exposure of ANSPs to potential Distributed Denial of Service (DDoS) attacks.

Network Information Security

2.3 Network Information Security requirements were described[1] as: IPv6, a Domain Name System (DNS), information security, network management and network contingencies.

2.4 The IATF envisions that the aviation community will inter-communicate using *IPv6 addresses*, from an ICAO block, so that aviation users can be identified. ICAO still has to fulfill its obligation to obtain such a block of addresses and allow the community to plan for their introduction.

2.5 Likewise, a secure *Domain Name System* (DNS) has been discussed for more than a decade but not yet materialized. DNS is essential to fulfill the Digital Identity concept.

2.6 *Information Security* applies to both data integrity and confidentiality. As previously mentioned, PKI Certificates can play a large role in this area but in the interim existing methods must be used:

- Sensitive data can be exchanged using IPsec tunnels, and that should always be the case when exchanging data over a public network.
- Incoming information should be scanned for malicious content by an edge device or firewall. This applies to information from existing trusted correspondents who may have been unknowingly compromised.
- Weather data is starting to be exchanged using ICAO Weather Information Exchange Model (IWXXM) encoded in Extensible Markup Language (XML). As an AMHS File Transfer Body Part (FTBP), this information payload will typically be scanned as part of the AMHS message information. Additional schema validation should be performed on the IWXXM data either programmatically or with a specialized security device. This is especially important since the IWXXM data may be compressed for FTBP exchange.

2.7 *Network Management* should isolate operational systems, networks and applications from public networks and other organizational devices by protecting them with security devices. Enterprise System Managers (ESM) should be used to monitor access and detect threats in real-time to allow mitigation responses.

2.8 *Network Contingency* should plan for normal failures and situations where systems or traffic has been compromised:

- Backup or disaster recovery systems should be implemented, preferably at a separate geographic site.
- Alternate data exchange routing should be planned, possibly using temporary IPsec tunneling over the Internet.
- Procedures should be developed for response to threat detection. Should access points be suspended? Should particular incoming information streams be stopped? Should applications be isolated? Can information be rerouted around a compromised correspondent?
- Communication channels between correspondents should be developed at multiple organizational levels in order to share details of an event and coordinate a response.
- What are the criteria for resuming normal information exchange?

System Wide Information Management (SWIM)

2.9 SWIM interchanges with external entities will typically contain XML formatted data (e.g. IWXXM, FIXM, AIXM). These exchanges can eventually be protected with Signing as a Service (SaaS) and Verifying as a Service (VaaS) using Digital Identities. In the interim:

- Information exchanges should be protected according to the network infrastructure used.
- Received XML information should be schema-validated either programmatically or with a specialized device.

2.10 A greater responsibility arises when SWIM services are used from a service provider because of a potential increase in the number of information providers or increase in the number of information consumers. In addition to the basic suggestions for SWIM data consumption, users should scan their published information prior to uploading to the service provider environment.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper; and

b) discuss any relevant matter as appropriate

– – – – – – – – – – – – –