International Civil Aviation Organization

Tenth Meeting of the Aeronautical Communication Services Implementation Coordination Group (ACSICG/10)

Bangkok, Thailand, 24 - 26 May 2023

Agenda Item 9: AFS related cyber-safety/security issues, best practices, and resilience

PROTECTING THE INTEGRITY AND EFFICIENCY OF CRV TIME-SENSITIVE EXCHANGES

(Presented by United States / FAA)

SUMMARY

This paper presents considerations for CRV information exchanges as CRV usage increases and evolves to support SWIM.

1. INTRODUCTION

1.1 ICAO's International Aviation Trust Framework (IATF) initiative proposes an environment where Digital Identities forms the basis of trust relationships for the secure exchange of digital information. Although comprehensive in its approach, implementation of the IAFT is still some way in the future. Bridging the trust authorities from different parts of the world will present implementation challenges. Meanwhile, world events continue to drive increased concern for the security of the telecommunications infrastructure.

1.2 The Asia Pacific Common AeRonautical Virtual Private Network (CRV) has been a success story for the Region, and encouraged greater inter-connectivity between the States than was previously practical and cost-effective with point-to-point technologies. Increased demand, and the future evolution to SWIM services, presents challenges to the efficiency of time-sensitive information exchange.

2. DISCUSSION

Defined Exchanges

2.1 The CRV was envisioned as a replacement for point-to-point circuits between participating ANSPs to support AMHS and voice service. In this network environment, practices associated with point-to-point circuits still make sense:

- Formalize the communication between parties with technical agreements clearly identifying the information to be exchanged.
- Identify and publish only the IP addresses necessary for the exchange and have agreements and procedures for changing them.
- Maintain GRE tunnels between network access points that codify the formal exchange agreements and limit visibility of end-user IP addresses to the intended parties.
- Address the required bandwidth for new information exchanges and whether adjustments to the contracted access bandwidth need to be considered.

Edge Protection

2.2 Although the CRV is a Virtual Private Network (VPN), users are still responsible for their cyber security to defend against threats.

- 'Security harden' network and application equipment.
- Deploy edge firewall devices at network connection points.
- Implement firewall rules and Access Control Lists (ACLs) that limit IP addresses to the very minimum necessary for information exchanges.
- Inspect exchanged data for malicious content. This applies to information from existing trusted correspondents who may have been unknowingly compromised.

Network User Governance

2.3 The CRV was envisioned as a private network between ANSPs for the support of Air Navigation Services. To continue its effectiveness, its use and users should be limited to the support of that mission.

- Manage the introduction of new network users and new services; non-ANSPs should require sponsorship by the ANSP with whom they will communicate.
- Use public networks (non-CRV) for public data distribution and non-essential data exchanges to limit ANSPs' cyber exposure.

Network Contingencies

2.4 States should plan for failures and situations where systems or traffic has been compromised:

- Backup or recovery systems should be implemented, preferably at separate geographic sites.
- Alternate information exchange routing should be planned, possibly using other networks or temporary IPsec tunneling over the Internet.
- Procedures should be developed for response to threat detection, including a decision to suspend a data exchange or reroute around a compromised correspondent.
- Communication channels between organizations should be developed, at multiple organizational levels, to share details of any event and coordinate a response.
- Criteria should be established for resuming normal information exchanges.

Migration to SWIM Information Exchanges

2.5 The recent decade has seen the migration of international information exchange from Aeronautical Fixed Telecommunications Network (AFTN) messaging, based on X.25 transport, to Air Traffic Services Message Handling System (AMHS) messaging based on IP transport. During this migration, ANSPs have operated in a mixed transport environment. Users have implemented AFTN/AMHS Gateways to accommodate older applications.

2.6 Weather data is beginning to be exchanged in XML-format, carried as the File Transfer Body Part (FTBP) of an extended AMHS message. Typically, there will be a period where legacy Traditional Alphanumeric Code (TAC) and XML format exchanges coexist as users adopt the new format.

2.7 Migration to SWIM data exchanges, between ANSPs, is expected to follow a similar pattern. SWIM exchanges for specific application functionality will coexist with older exchange technologies. Translation between SWIM and legacy formats will be available, e.g. the AMHS/SWIM gateway being formalized in the European SWAMWAY initiative.

Information Transport Priorities

2.8 Current voice and data exchanges over CRV have different transport processing defined by Differentiated Services Code Point (DSCP) markings in their IP headers. Voice traffic uses an Expedited Forwarding ('EF') marker to achieve priority processing. AMHS traffic uses a Low Latency Data marker ('AF21') for lower priority processing but with a low drop probability.

2.9 To avoid interaction between AMHS and SWIM data flows, additional DSCP markers could be used to determine the desired transport processing according to the SWIM application functionality. It is suggested that this topic be addressed by the CRV Governance Group.

SWIM Information Security

2.10 Confidentiality and integrity of legacy information was ensured by the fact that point-to-point circuits were inherently private connections. With the CRV, the network continues to be private but there is exposure to more users. Some confidentiality is provided by GRE tunnels. With the introduction of SWIM exchanges, there is the opportunity to address confidentiality and integrity requirements before implementation rather than as an afterthought. It is recommended that this be addressed by the SWIM Task Force.

SWIM Evolution Summary

2.11 In summary, consider the following for the introduction of SWIM traffic:

- Use agreements to formalize the exchange of information
- Continue the use of GRE tunnels between network access points
- Consider whether extra bandwidth is needed to support the SWIM traffic
- Consider whether functionality for data integrity and confidentiality can be built into the SWIM information exchanges before implementation.
- Determine what DSCP codes should be used for network transport processing
- Address traffic contingencies for failure or compromise scenarios

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

– – – – – – – – – – – – –