International Civil Aviation Organization

Twenty Fifth Meeting of the Communications/ Navigation and Surveillance Sub-group (CNS SG/25) of APANPIRG

Video Tele-Conference, 18 – 22 October 2021

Agenda Item 11: Cybersecurity of CNS/ATM systems

11.1 Review outcomes of ICAO Cyber Security Webinar

IMPLICATIONS OF CYBERSECURITY AND ASSOCIATED REQUIREMENTS FOR CRV OPERATIONS

(Presented by United States)

SUMMARY

This paper reviews the current and envisioned future environments for CRV operations to provide a framework for discussion of requirements for Cyber Security and SWIM.

1. INTRODUCTION

1.1 This paper addresses the implications for existing services and the Asia Pacific Common AeRonautical Virtual Private Network (CRV) resulting from the recent Cybersecurity Webinar[1]. For the future, it addresses support of SWIM and other proposed services for the Region.

2. DISCUSSION

Point-to-Point Connections

2.1 The Aeronautical Fixed Service (AFS), as specified in ICAO Annex 10, has traditionally provided voice and data connections over point-to-point telecommunications. With the migration towards the IP-based Air Traffic Services Message Handling System (AMHS) and Voice over Internet Protocol (VoIP), as specified on ICAO Docs 9880 and 9896 respectively, these services can now be carried by IP transport over the more flexible CRV yet still be configured as limited point-to-point connections.

2.2 These point-to-point connections and associated information flows result from, and are enforced by, functionally dedicated systems such as flight processing, weather and NOTAMs.

---

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

System Wide Information Management (SWIM)

2.3 System Wide Information Management (SWIM) "*shifts the ATM information architecture paradigm from point-to-point data exchanges to system-wide interoperability*."[2]

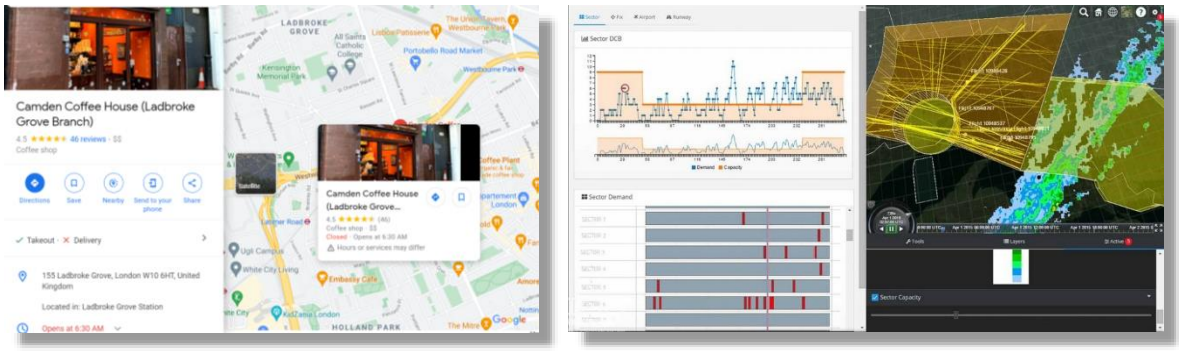
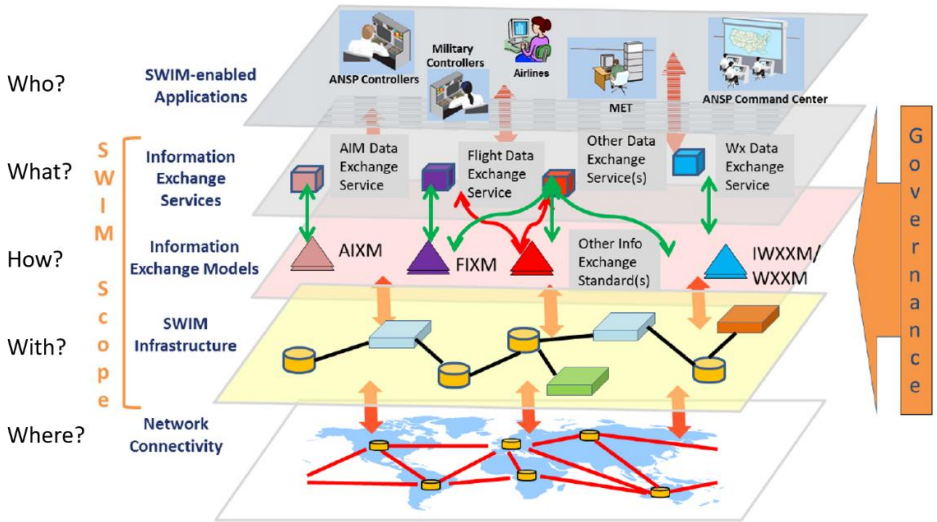


Figure 1: Google "mash up" similarity to ATM fused display.

We are familiar with "mash-ups" in Google Maps that conveniently combine information from multiple sources. SWIM, likewise, aims to support applications that combine useful information in the ATM environment, as illustrated in Figure1. The ATM Operational Concept envisages that, "*information management solutions will be defined at the overall system level, rather than individually at each major subsystem (programme/ project/ process/ function) and interface level*."[3] Rather than the subsystem defining the display, the paradigm is changed so that the desired display defines the information requirements from subsystems.



Information Exchange Services defined for each ATM information domain and for cross domain purposes, where opportune, following governance specifications and agreed upon by SWIM stakeholders. SWIM-enabled applications will use information exchange services for interaction;

Information Exchange Models using subject-specific standards for sharing information for the above Information Exchange Services. The information exchange models define the syntax and semantics of the data exchanged by applications;

SWIM Infrastructure for sharing information provides the core services such as interface management, request-reply and publish-subscribe messaging, service security, and enterprise service management.

Figure 2: SWIM Five Layer Architecture

[2] Manual on System Wide Information Management (SWIM) Concept, ICAO Doc 10039.
[3] Global Air Traffic Management Operational Concept, Doc 9854

2.4 Broadening access in an IP environment beyond limited point-to-point connections can increase exposure to malicious infiltration. Central to mitigating this threat is verifying the legitimacy of "who" is accessing the infrastructure and "what" information they are entitled to. The recent Cyber Security Webinar presented the work of the International Aviation Trust Framework (IATF) initiative The IATF is composed of *Digital Identity* and *Network Information Security* elements.

Digital Identity

2.5 Digital Identity declares who or what you are by providing a credential to that effect to a given level of assurance. Work on Digital Identity is focused on Digital Certificates that use Public/Private key encryption to support a hierarchy of certificate verification.

[[[Root CA] Intermediate-CA] User]

A trusted Root Certificate Authority (CA) provides a self-signed certificate and signs a certificate for a verified Intermediate CA. The latter includes that credential when issuing a signed certificate for a verified User. The User can then present this 'nested' certificate when requesting access. The target must be able to verify all signatures in this presented certificate credential and so must have access to data about these CAs and any revocations (invalidated certificates). Challenges remain in expanding this concept to a global environment where there may be multiple trust roots. Note that China has proposed[4] an interesting alternative solution to root trust using block-chains.

2.6 A common naming system must be adopted for use by all the entities that are likely to inter-communicate, e.g. authorities, ANSPs, service providers, manned and unmanned aircraft. Where needed, a Domain Name System (DNS) must translate names into IP addresses.

2.7 Today's AMHS systems uses simple authentication credentials when connecting across the CRV. Digital Identity certificates can be used instead. VoIP can be secured similarly.

2.8 ICAO has stated that Digital Identity is required for SWIM connections. Identity verification is a function of the SWIM infrastructure layer, shown in Figure 3, which is also responsible for data integrity.

Figure 3: SWIM Layered Functionality

[4] SP/203 – "A method of building global mutual trust infrastructure based on blockchain", Asia/Pacific Regional Cybersecurity webinar: *"Management Framework/or CNSIATM Systems"*, 14 June 2021

Management of Digital Identities is the responsibility of each network User; it is not a function of CRV. The latter, however, may need to provide the transport for verification.

Network Information Security

2.9 Network Information Security requirements were presented as: IPv6 (dedicated ICAO block); Domain Name System (DNS); information security; network management and network contingency plans.

2.10 IPv6 support directly affects CRV implementations and requires planning.

2.11 DNS translates names of connection targets into IP addresses and supports common naming. The CRV needs to support transport and distribution of DNS. Non-ANSP access may be required. Users may have to provide local DNS caching.

2.12 Information security addresses the requirements for information confidentiality, integrity and availability. In general, these are expected to be requirements for Users rather than the CRV network. Naturally, when traversing the Internet or other Public domains, encrypted tunnels are recommended to prevent intrusion.

2.13 Network management and network contingencies suggests monitoring and intelligent use of the User's networking ecosystem including access across CRV to any 'cloud services'. It does not suggest additional monitoring by the CRV service provider.

SWIM

2.14 SWIM has two separable concepts: information services in a service-oriented architecture (SOA); and information consolidation from multiple sources.

2.14.1 With well-defined SWIM services (documented in a registry), a User's information can be provided to many requesters. Similarly, the User can obtain information from multiple sources. This results in many to many (federated) connections.

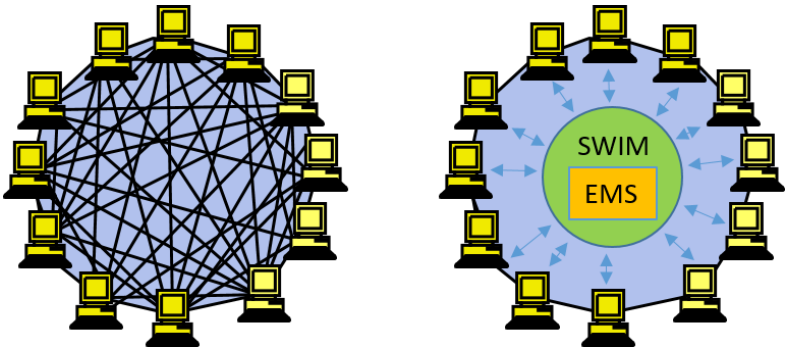


Figure 4: Federated and Centralized SWIM Architectures

2.14.2 Rather than each User have many connections, Users can supply their information to a centralized SWIM Enterprise Management System (EMS) that supplies recipients with combined information in a consolidated delivery. This minimizes the connections and bandwidth usage of the network. The EMS acts as an information switch. Additional mediation services or applications can be offered from this centralized platform.

SWIM as a Service

2.15 An Information Paper[5] for the SWIM Task Force by PCCW (the CRV service provider) offered SWIM as a service (SWIM Infrastructure and Information Exchange Services accessible over the network) for Users not wishing to invest in a local SWIM implementation.

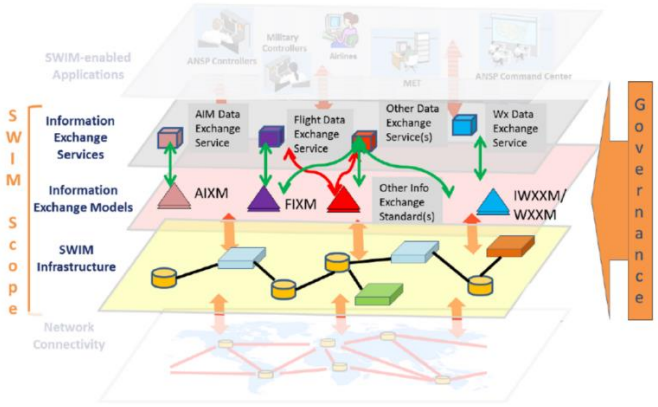


Figure 5: Scope for SWIM as a Service

A User's local client applications could access hosted SWIM Information Exchange Services over the CRV. The hosted SWIM environment may interact with other SWIM deployments and information sources and could provide information consolidation and mediation services, e.g. translation from Traditional Alphanumeric Code (TAC) to ICAO Weather Information Exchange Model (IWXXM).

2.16 Integration of SWIM as a Service effectively extends the User's network ecosystem. All the considerations of Digital Identity and Network Information Security are applicable.

3. IMPLICATIONS AND CHALLENGES

Implications

3.1 Adoption of Cyber Security would suggest the following requirements:

3.1.1 ICAO Requirements

a) ICAO needs to provide an IPv6 dedicated address block

b) ICAO needs to propose a Name Space and field a DNS

c) ICAO needs to deliver IAFT recommendations for security including a Trust Framework for Digital Identities

3.1.2 CRV Network Requirements

d) CRV needs to plan to implement IPV6

e) CRV needs to provide transport for DNS access and distribution

[5] Information Paper (IP/07) of the Asia Pacific Fourth Meeting of System Wide Information Management Task Force (SWIM TF/4), November 2020.

f) CRV needs to provide transport for Digital Identity verification

3.1.3 Service Provider Options

g) Service Providers may offer optional SWIM services and applications to Users.

3.1.4 CRV User Requirements

h) CRV Users need to implement network security

i) CRV Users need to plan for IPv6 implementation

j) CRV Users need to plan to support ICAO naming and DNS

k) CRV Users need to plan to adopt Digital Identities, as prescribed by ICAO, and use them in connections to SWIM services

l) CRV Users may implement SWIM, may access SWIM as a service, or may adopt some hybrid of the two.

m) CRV Users may implement data integrity using digital signing

Challenges

3.2 Addressing Cyber Security and SWIM poses some questions and challenges:

3.2.1 Which body will provide continuing management of the DNS namespace? Perhaps something similar to the ATS Messaging Management Centre (AMC) is needed.

3.2.2 Shared SWIM services will initiate the exchange of information between an ANSP and a Service Provider rather than one-way information receipt (e.g. Aireon ADS-B data). Before SWIM Services are offered, should there be an agreement that the Service Provider will conform to any ICAO security recommendations, provide SWIM services in accordance with any ICAO Standards and Recommended Practices (SARPS), and provide an agreed service level. Which body should enter into such an agreement, execute some governance and oversee the service provision?

3.2.3 Shared SWIM services can lead to the exchange of information between ANSPs through provision of a Global Enterprise Messaging Service (GEMS). How should competing GEMS within a region be prevented? How should information be efficiently distributed such that ANSP information providers are not overtaxed in bandwidth demands?

3.2.4 As part of the Aeronautical Telecommunication Network (ATN), the existing private CRV transports voice and time-critical data. As time-critical information flows move to SWIM, they should also use the ATN but SWIM carries a much greater bandwidth of advisory information that is not time-critical. Carrying the latter over a private network may be cost-prohibitive for many ANSPs. Guidelines for sensible use of the ATN and the Internet for SWIM information is needed.

4. ACTION BY THE MEETING

4.1 The meeting is invited to embrace Cyber Security and take note of these suggested implications and challenges.

– – – – – – – – – – – – –