MIDANPIRG/16-WP/37
09/02/2017

International Civil Aviation Organization

Middle East Air Navigation Planning and
Implementation Regional Group

Sixteenth Meeting (MIDANPIRG/16)
(Kuwait, 13 – 16 February 2017)

Agenda Item 5.2.2: Specific air navigation issues

ATM DATA SECURITY

(Presented by United Arab Emirates)

SUMMARY

The purpose of this working paper is to present the challenges that are faced by all ANSP's within the region with respect to the safeguarding of data and system integrity.
These issues are common amongst all states and it is our responsibility as service providers to protect the ATM data and systems as best as possible.

Action by the meeting is at paragraph 3.

REFERENCES

- Annex 17 – recommendation for states on Cyber threats
- Doc 9985 - Air traffic management security manual
- Doc 8973 – Aviation security manual – Chapter 18

1. INTRODUCTION

1.1 Data security in ATM as the name suggests is the safeguarding of data from malicious/targeted attacks for both ground-ground communications as well as air-ground communications.

1.2 This working paper is looking into its impact, what the UAE is doing in this regard and what measures can be taken within the region to safeguard the systems from attacks.

2. DISCUSSION

2.1 With the amount of data being transferred via internal and external networks at present there is an enormous attraction for organized hostile entities such as hackers, terrorist, unfaithful employees, business competitors, foreign state etc. to infiltrate or intercept a network for various reasons such as:

2.1.1 Terrorism
2.1.2 Vandalism
2.1.3 Financial gain
2.1.4 Corporate or state espionage

2.2 The following table illustrates the causes, threats and impact of the above mentioned:

CAUSES	THREAT	IMPACT
Hackers	System/network access	Malicious data usage Personal data theft Blackmail System degradation
Terrorists	Credible corruption of data GPS Spoofing ADS-B Spoofing Navaids disruption Network disruption RF interference/jamming	Malicious operations Incidents due to corrupted data Diverted traffic Airspace disruptions Accidents
Suppliers	Supply chain risks	Backdoor access for information gathering System performance
Unfaithful employees	Unauthorized access (Physical/Network)	Blackmail Personal data distribution Vandalism
Business competitors	Targeted attacks	Traffic restrictions/diversions System degradation
Foreign state	DDoS attacks ATM system disruptions RF interference/jamming	Service disruptions Airspace closures

2.3 Of course there are many more reasons however any one of the threats in the table in 2.2 is an unwanted issue and the simple fact is with our ever evolving ATM systems, including the respective AIM data and systems, ANSP's are becoming more vulnerable to cyber-attacks.

2.4 The ICAO ASBU's have been put in place to facilitate the global harmonization of ATM systems. With the need for more "system-to-system" interoperability there is no doubt that the performance of the ATM system as a whole will improve. This however will also increase our reliance on automation and IP connectivity which leaves us vulnerable if we are not adequately protected.

2.5 The SWIM concept is an integral part of the ASBU's and proper planning should be done to ensure that when inter-system connectivity is required it is secure, easy to configure and scalable for future developments.

2.6 Air transport is heavily dependent on aircraft/system driven information and the SWIM concept requires communication not only within the state and adjacent units but with all the respective stakeholders involved in Gate to Gate operations. For example the securing of air to ground communications should be a collaborative effort between the airlines and the ANSP's.

2.7 A compromise to the GPS signal, corrupted downlink data, hacked ground systems, spoofed data, RF interference/jamming etc. could have a massive effect on our daily operations. Security of IT infrastructure has been around for a long time now, however ATM system specific equipment is limited.

2.8 While there is no network in existence that is 100% secure the SWIM requirements require ATM systems to be connected to the internet or other data networks. Bearing this in mind ANSP's need to adopt a proactive approach to the cyber threat as this is the only way we will be able to safeguard not only the data we are currently using but also the future requirements.

2.9 Considering the amount of threats faced in the cyber world, GCAA is constantly assessing its ATM security to determine the deficiencies and ensure that a comprehensive plan is in place to best protect the ATM system.

2.10 Bearing this in mind GCAA has installed a 3 factor authentication security system for its ground to ground communication which will be entry and exit point to our systems once fully operational. The main function of this security setup will allow remote access to a dedicated "zone" within our network based on 3 different authentication methods.

2.11 For ground to air communications GCAA works closely with the TRA on issues related to the interference of our RF spectrum. GCAA has multiple remote VHF sites which are connected via our IPVPN network back to our ACC/EACC. These sites are connected either by E1 or VoIP and provide us redundancy in frequency availability. Encryption on WAN links is also in place to best protect our data streams.

2.12 While all this is in place we are constantly looking at ways to improve the resilience of the ATM system as new threats will always be there. The financial aspect of these measures is substantial however to ensure safe operations it is our responsibility to ensure adequate protection is in place.

2.13 With the MID region looking at the viability of a dedicated Common Regional Virtual Private Network (CRV) we could/should not only use the APAC regions model as the basis for our network design but also benchmark our network planning against what is already in place in the USA and EU.

2.14 As this network will be the enabler of SWIM, forming the backbone of the ground to ground communications within the MID region, a dedicated SOC responsible for planning, monitoring and incident management must be in place with staff from the aviation field as conventional IT standards are different to the standard required in Aviation.

2.15 The impact of a compromised system could ultimately lead to the loss of life and it is each and every ANSP employee's responsibility to do their part in keeping the ATM system safeguarded as best as possible.

2.16 The safety culture that exists in our day to day operations is there because we all buy into the fact that safety is critical and that there is no compromise on this. In the same way we should all buy into a "security culture" where data protection is paramount to our day to day operations.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information in the paper and take action as appropriate related to the MID CRV implementation;

b) consider the establishment of the MID Region ATM data security plan that; and

   i. Defines the minimum requirements needed to protect the ATM data security.

   ii. Defines the system architecture relevant to each state

   iii. Defines a test and implementation schedule/plan

c) require states to mandate a clear and concise strategy on ATM data security and resilience

- END -