INTERNATIONAL CIVIL AVIATION ORGANIZATION
ASIA AND PACIFIC OFFICE

GUIDANCE MATERIAL: SECURITY ISSUES ASSOCIATED WITH ADS-B

GUIDANCE MATERIAL: SECURITY ISSUES ASSOCIATED WITH ADS-B

1. Statement of issue

1.1. ADS-B technologies

All ADS-B technologies are currently defined as “open systems”. The data, including position and flight identification are broadcast by aircraft and can be received by any airborne or ground based receiver. The signal and transmitted data are fully standardised and those standards are public. This situation is not specific to ADS-B and is very similar for other civil aviation CNS technologies.

It can also be noted that ADS-B transmission from commercial aircraft is a “fact of life” today. Many commercial aircraft are already equipped with ADS-B and have been transmitting data for some time.

1.2. Publicity

In some states, there has been considerable alarmist publicity regarding ADS-B security. To a large extent, this publicity has not considered the nature and complexity of ATC. Careful security assessments and security policies in use today for ADS-B and other technologies can provide a more balanced view.

1.3. ICAO ANC

The ICAO ADS-B Concept of Use as presented to ANConf/11 (AN-Conf/11-WP/6) has a number of paragraphs relating to security namely para 4.2.7 and 5.2.4. These include:

> *"There are practical limits that must be recognized due to technological, political, and fiscal reasons. Not all solutions will be technical, that is, come from a box. Some of the solutions may be procedural, legal, technical or a combination of all. In short, States will need to consider the likelihood and severity of interference by conducting appropriate hazard and safety assessments as a means of developing mitigation strategies*."

1.4. Availability of receivers & emitters

The ADS-B technology is quite simple and the development of a receiver or an emitter does not require exceptional expertise or very expensive hardware. This is the cornerstone of affordable lower cost air-ground and air-air surveillance**.**

The complexity of secondary radar is higher than ADS-B and it is more difficult to get an accurate traffic display through a home made radar or multilateration system.

Low cost ADS-B 1090 MHz receivers for personal use are available on the market and can be connected to a standard PC. It is thus possible to display an air traffic situation in real time at any private location.

Emitting false traffic information from a ground location is also feasible.

1.5. Potential Vulnerabilities

The following provides a brief discussion of some identified vulnerabilities. Knowing these threats, each State has to consider the potential impact, and when required, the appropriate counter-measures in order to mitigate the identified risks or consequences.

It can be noted that the EASA ADS-B certification document (AMC 20-24) recommends that ADS-B transmission can be switched off by the pilot. If available, this capability can be used as needed in sensitive areas or for special flights, in negotiation with ATS.

It can also be noted that legislation and associated enforcement can be applied to provide some mitigation against some risks.

1.5.1. Confidentiality

Confidentiality is the property that information is accessible only to those authorized to have access. However, this needs to be balanced against a significant intent of ADS-B; namely to allow all airspace users have visibility of all other airspace users. Therefore low cost and ease of reception is one of the key benefits to be delivered. As a result, some aspects of "privacy" may be lost.

Control and/or restrictions on the use of ADS-B receivers and broadcast of ADS-B data on the Internet could also be considered.

Some of the identified threats are shown below.

	CONFIDENTIALITY	
Issue		**Considerations**
1	Flight number and position of aircraft are available to the public	Procedures to support sensitive flights to use different flight identities. Allow "privacy" modes eg: flight ID as "VFR" For special needs use DF19 encrypted ADS-B transmissions.
2	Unique 24 bit code identifies the aircraft and is available to the public.	Procedures should be developed, if required, to support sensitive and military flights. Allow use of different 24 bit codes for special flights if required
3	Use of position and aircraft ID data for the coordination of attacks against specific airborne targets (e.g. VIP)	These specific flights should have the capability to switch off ADS-B and be managed in special ways
4	Use of position and aircraft ID data for economic intelligence: surveillance of business aircraft or commercial aircraft	Procedures to support sensitive flights to use different flight identities.
5	Re-transmission via Internet	Legislative controls on retransmission could be considered but likely to be ineffective

1.5.2. Integrity

Integrity is the property that data cannot be created, changed or deleted without authorization.

	INTEGRITY	
Issue		**Considerations**
1	False messages: transmission of false messages from virtual aircraft (spoofing); risk of false alarms (STCA), false traffic information, spurious separation manoeuvres.	ATC operates not just using surveillance but correlate the surveillance picture with voice communication, the flight plan, controller expectations of "normal behaviour If related risks warrant it (especially in high density environments) additional functions can be provided to warn and protect ATC. ATC system protections can include : - schemes to match surveillance tracks with current flight plan data state including position, route, level, identity etc - Alerting if the ADS-B track is outside route and vertical clearance limits - Ability to decouple misleading data from a flight plan - Detection of positional data "jumps" (reasonableness checking) - Warnings of potentially misleading data o Duplicate matches to a flight plan o Duplicate 24 bit codes o Duplicate FlightID on different targets - Not coupling ADS-B track data to a flight plan if the track arrives into coverage at an unexpected position or arrives into coverage at an unexpected time, or without co-ordination Ground station considerations could include the following at additional cost - Use of direction finding capabilities to validate the "quadrant" from which the data is received - Use of active SSR ranging to validate the range of the aircraft Use of SSR, primary radar or multilateration Automated tools to warn controllers of this potential hazard.

	INTEGRITY	
Issue		**Considerations**
2	Alteration of messages during their transmission between the ground stations and the ATM system	Appropriate protections are required for the security of ADS-B transmission network between Ground station and ATC centre
3	Deleted messages: possible loss of aircraft visualisation on controller display	Appropriate protections are required for the security of ADS-B transmission network between Ground station and ATC centre. Effect is somewhat identical to avionics failure. Procedures are in place to manage this event.

1.5.3. Availability

Availability is the property that aircraft information is available to the ATM system/unit when needed

ATM systems and controllers typically have processes to be used following loss of surveillance and other information. These should take into account possible loss of ADS-B information for both malicious and inadvertent or accidental outages.

	AVAILABILITY	
Issue		**Considerations**
1	Jamming of a receiving ground station by transmission of a high power signal on 1090 MHz	Effect is somewhat identical to ground station failure. Procedures are in place to manage this event.
2	Jamming of GPS in a particular geographical area denies the positional data	Effect is somewhat identical to ground station failure. Procedures are in place to manage this event. Avionics are becoming available that meld GPS with inertial positional data to coast through.
3	Transmission of a large amount of false messages in order to saturate the channel of ground system data processing, or the ATCO surveillance display (spoofing)	Effect is somewhat identical to ground station failure. Procedures are in place to manage this event. Protections could include : - Ability to disconnect an ADS-B ground station (eg if data flooding occurs) so to limit loss to a single sensor - Filtering ground station data based on range, on SIC/SAC, on 24 bit codes

2. Recommendations

2.1 While ADS-B is recognized as a key enabling technology for aviation with potential safety benefits, it is recommended that States are aware of possible ADS-B security specific issues.

2.2 It is recommended that States note that much of the discussion of ADS-B issues in the Press has not considered the complete picture regarding the ATC use of surveillance data.

2.3 For current ADS-B technology implementation, security risk assessment studies should be made in coordination with appropriate state organisations and ANSPs to address appropriate mitigation applicable in each operational environment, in accordance with ATM interoperability requirements.

2.4 Future development of ADS-B technology, as planned in the SESAR master plan for example, should address security issues. Studies should be made to identify potential encryption and authentication techniques, taking into consideration the operational need of air to ground and air to air surveillance applications. Distribution of encryption keys to a large number of ADS-B receivers is likely to be problematic and solutions in the near and medium term are not considered likely to be deployed worldwide.

– – – – – – – – – – – –