ADS-B CYBER SECURITY ALERT

JOHN PERKAUS | 2020

ADS B PRIVACY CYBER SECURITY ALERT ADS-B IS MANDATED IN ALL AIRCRAFT ON JANUARY 1, 2020

The Automatic Dependent Surveillance-Broadcast (ADS-B) tracking tool provides real- time information on an aircraft's location, velocity and airframe dimensions.

HOW ADS-B WORKS: AUTOMATIC DEPENDENT SURVEILLANCE BROADCAST

- Uses GPS and Radio Frequency (RF) data link to broadcast twice per second the aircraft information to airborne and ground receivers,
- The source of position information is provided by GPS system.
- The aircraft has a transmitter, receiver and a processing device, which receives information from the GPS, and the Flight Management System (FMS) to provide an image to the pilot on the cockpit display.
- The FMS gives information about the flight plan, ensures the correct trajectory of the aircraft, and automates procedures when the aircraft is airborne
- The GPS sensors and FMS provide information to the transmitter to broadcast surveillance data to the other aircrafts and to the ground stations
- The ground station executes the same process to display the information on the respective screen and, thereafter to broadcast the air traffic information

ADS-B DESIGN ISSUES PROBLEMS & VULNERABILITIES

ADS-B was designed without encryption/other security measures and its vulnerabilities have not been addressed/mitigated.

ADS-B Vulnerabilities

- Confidentiality of information transmitted through ADSB channel
- Integrity of information transmitted with the ADS-B messages
- Communication availability with ADS-B

ADS-B SECTORS OF VULNERABILITY:

Ground Sector

- ADS-B ground networks, including data link and ground stations
- Distributed computer networks
- ATC ground control station

Air Sector

- Onboard aircraft ADS-B system

Air-Ground Sector

- Data broadcast communication medium ADS-B

ADS-B CYBER SECURITY ALERT

JOHN PERKAUS | 2020

ADS-B ATTACK METHODS:

- Interception and monitoring of ADS-B OUT signals, message injection, jamming of GPS and RF signals, Ghost Aircraft message deletion, message modification

INTERCEPTION AND MONITORING OF ADS-B OUT SIGNALS

Anyone with a commercially available ADS B receiver can conduct aircraft monitoring, reconnaissance/eavesdropping.

-Attack Type: Signal Interception - conduct aircraft monitoring, reconnaissance, eavesdropping of ADS-B.
  - Target Sector: air-ground sector.
  - Attack Technique: Interception of ADS-B OUT.
  - Technical Difficulty: Low.
  - Impact: The attack does not produce any direct impact to the aviation system.

MESSAGE INJECTION

Takes various forms: jamming of GPS/RF signals, Ghost Aircraft, and Aircraft Spoofing

- Attack Type: Jamming of GPS and RF signals - Hackers transmit an unmanageable amount of messages in order to saturate the channel resulting in disabling one or more nodes in the wireless network from sending or receiving messages with enough power to disrupt GPS or RF radio frequency signals
  - Target: Air segment and air-ground segment.
  - Attack Technique: Jamming that disrupts RF channel and/or GPS signals transmitting to A/C.
  - Technical Difficulty: Medium
  -Impact; possibly severe in congested air spaces and adverse weather conditions

- Attack Type: Ghost Aircraft – Hackers inject aircraft with credible data so the receiver cannot detect the "ghost" as fake.
  - Attack Technique: insertion of message containing credible date which appears to pilots as real aircraft
  - Technical Difficulty: Medium-High.
  - Impact: Severe – pilots increase of workload while trying to identify by other means a possible real aircraft, which may interfere with trajectory.

- Attack Type: Aircraft Spoofing – Hacker combines message injection and message deletion in attack
  - Attack Technique: attacker eavesdrops on RF channel in order to interpret the messages and to interfere with the required message [52].
  - Target: Ground segment and air-ground segment.
  - Attack Technique: Message Deletion, message injection and interception of ADS-OUT.
  - Technical Difficulty: Medium
  - Impact: Most severe increase the workload of the air traffic controllers

ADS-B CYBER SECURITY ALERT

JOHN PERKAUS | 2020

- Attack Type: Message Deletion Ground Station Target Ghost Inject Hackers – inject a single "ghost aircraft" in the ground station of the air traffic control.

    - Attack Technique: use of constructive interference to delete messages from the wireless network, then hackers injects a single "ghost aircraft" in the ground station of the air traffic control.
    - Target: Ground segment and air ground-segment.
    - Technical Difficulty: Medium-High – attacker must know the proper data contained in an ADS-B message for legitimate flights in order to create the ghost aircraft.
    - Impact: Most Severe – significantly increases ATC personnel workload

MESSAGE MODIFICATION

The integrity of the message is affected with the modification of the information contained in the message

- Attack Type: Overshadowing – modify the message by overshadowing the signal since it is easier for the attacker to decode the message without error.
    - Attack Technique: the attacker must correctly time and position himself for sending message modification.
    - Technical Difficulty: High

- Attack Type: Bit-flipping – modify the message by revising content; intercept, decode, and resend message
    - Attack Technique: attacker must correctly decode, time and position self for sending of message modification
    - Technical Difficulty: High

CONCLUSIONS

- With US implementation of ADS-B in a few short months, aviation stakeholders will be subjected to new and unforeseen privacy and cybersecurity risks.

- To prepare for ADS-B all U.S. aviation stakeholders should invest in employee training on privacy, cybersecurity system vulnerabilities, potential attack recognition, and remediation procedures.