Civil Aviation Cyber Threats

Tom Alexandrovich
Aviation Guidance Manager

Security Vulnerabilities in Next Generation Air Transportation Systems
DISCLAIMER

• This presentation is for informational purposes only.
• Do not apply the material if not explicitly authorized to do so
• I’m taking full responsibility whatsoever of applying or experimenting with presented material
• Authors are fully waived of any claims of direct or indirect damages that might arise from applying the material

• DO NOT TRY THIS AT HOME!
• USE AT YOUR OWN RISK!
Is any one a pilot?
Civil Aviation Cyber Security
Major Cyber Threats in Aviation

- **Downing An Airplane**
  Damage to vital systems for aircraft flying
  Disrupting information and changing data that will cause pilots to make "wrong decisions".
  Disrupting information that would cause a false representation that would force the pilots to land the aircraft.

- **Disabling The Airport**
  Airport Closure
  Taking control of a system that will cause "public trust" damage.
Cyber Events In Aviation

- Disruption of GPS systems of unmanned aircraft
- Penetration into ground computing systems
- Penetration of aircraft systems through a computer interface in the passenger compartment
Cyber Threats - Airport

- Damage to the Runway Lighting System
- Disruption of HBS baggage system
- Disruption of the HVAC system, electricity or parking
- Jamming ramps or sleeves
- Access to physical security systems
- A ransom attack
CONNECTED AIRCRAFT
Cyber Threats - Cockpit

- Attack vectors based on penetrating aircraft systems
- Software update
- Communication channels
- Updating the EFB
Cyber threats - Ground Systems

Attack vectors through ground systems

- Operating networks of airlines
- Supply chain: software or hardware
Cyber Threats - Passenger Cabin

Attack vectors through passenger cabin

- Disruption of aircraft systems through cabin interfaces
- Exposure to Improper content in the multimedia system
- Lack of monitoring or supervision of access points and connection from the passenger cabin
- Theft of personal information
Supply Chain

787 Dreamliner structure suppliers

- **Part name**
  - **Company (country)**
- **Movable trailing edge**
  - (U.S., Canada, Australia)
- **Horizontal stabilizer**
  - Alenia (Italy)
- **Tail fin**
  - Boeing (U.S.)
- **Rear fuselage**
  - Boeing (U.S.)
- **Wing-to-body fairing**
  - Boeing (U.S.)
- **Passenger entry door**
  - Latecoere (France)
- **Lithium-ion batteries**
  - GS Yuasa (Japan)
- **Main landing gear wheel well**
  - Kawasaki (Japan)
- **Engine nacelles**
  - Goodrich (U.S.)
- **Engine**
  - Rolls-Royce (U.K.)
- **Fixed trailing edge**
  - Kawasaki (Japan)
- **Forward fuselage**
  - Spirit (U.S.)
- **Centre wing box**
  - Kawasaki (Japan)
- **Landing gear structure**
  - Messier-Dowty (France)
- **OTHERS**
  - Wing/body fairing
    - Boeing (Canada)
  - Cargo access door
    - Saab (Sweden)

**Suppliers**
- **Supply Chain**
Cyber Threats - Aircraft Connectivity

- ADS-B
- ACARS
- SATCOM
- VHF
- WIFI

Cyber Israel
Automatic Dependent Surveillance-Broadcast
ATC of the future (FAA NextGen project)
Required on most AC in US by 2020, required in Europe

Augments primary surveillance radar (ADS-B Out)
Gives pilots their own radar picture (ADS-B In)
Transport layer, not physical (OSI level 4)
ADS-B System
Automatic Dependent Surveillance Broadcast

• Replacing radar for tracking aircraft worldwide
• Sharing position, altitude, velocity, etc. with air traffic control and other aircraft

Advantages:
• Increased situational awareness
• Coverage in areas without radar
• Less Expensive

Broadcast Message:
- Position, altitude, airspeed, identification, category, climbing, descending, turning
- Receive broadcast data from all aircraft
- Receive GPS-data
How ADS-B Works

Disadvantages:
• Not secured
• Easily accessible
ADS-B Input Mistakes

When making routine code changes, you should avoid inadvertent selection of codes 7500, 7600, or 7700 thereby causing momentary false alarms at automated ground facilities. For example when switching from code 2700 to code 7200, switch first to 2200 then 7200, NOT to 7700 and then 7200.

Important Codes

- **1200** — The VFR Code for any altitude.
- **7600** — Loss of Communications.
- **7500** — Hijacking (Never assigned by ATC, her aircraft is subject to unlawful interference).
- **7700** — Emergency (All secondary surveillance times).

### Important Codes

Following is a list of important codes:

- **1200** — VFR code in the U.S. (refer to ICAO standards for VFR codes in other countries).
- **7600** — VFR code commonly used in Europe (refer to ICAO standards).
- **7500** — Hijack code.
- **7600** — Loss of communication code.
- **7700** — Emergency code.
- **7777** — Military interceptor operations code (NEVER SQUAWK THIS CODE).
- **0000** — Code for military use in the U.S.
Decreased Separation Distance

Without ADS-B Coverage

One In, One Out

20 NM

With ADS-B Coverage

Separation distance decreased to 5 NM

5 NM  5 NM  5 NM  5 NM
ADS-B Out VS ADS-B In

**ADS-B Out** is the broadcast part of ADS-B. An aircraft equipped with ADS-B Out capability will continuously transmit aircraft data such as airspeed, altitude, and location to ADS-B ground stations.

**ADS-B In** is the receiver part of the system. ADS-B In equipment allows aircraft, when equipped properly, to receive and interpret other participating aircraft's ADS-B Out data on a computer screen or an Electronic Flight Bag in the cockpit.
Surveillance Coverage

Radar and ADS-B coverage

Only ADS-B coverage
ADS-B Security?

✈ None at all

✈ Attacks range from passive attacks (eavesdropping) to active attacks (message jamming, replaying, injection).

✈ Target selection
» Public Data
» Local data (SDR*)
» Virtual Aircrafts
# Attacks and Affected Assets of ADS-B

<table>
<thead>
<tr>
<th>THREATS</th>
<th>AFFECTED ASSETS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confidentiality</td>
</tr>
<tr>
<td>Aircraft Reconnaissance</td>
<td>X</td>
</tr>
<tr>
<td>Aircraft Target Ghost Inject</td>
<td>X</td>
</tr>
<tr>
<td>Ground Station Target Ghost Inject</td>
<td></td>
</tr>
<tr>
<td>Ground Station Multiple Ghost Inject</td>
<td></td>
</tr>
<tr>
<td>Replay Attack</td>
<td>X</td>
</tr>
<tr>
<td>Aircraft Spoofing</td>
<td>X</td>
</tr>
<tr>
<td>Virtual Trajectory Modification</td>
<td>X</td>
</tr>
<tr>
<td>Aircraft Disappearance</td>
<td>X</td>
</tr>
<tr>
<td>False Alarm Attack</td>
<td>X</td>
</tr>
<tr>
<td>Aircraft Flood Denial</td>
<td></td>
</tr>
<tr>
<td>Ground Station Flood Denial</td>
<td></td>
</tr>
</tbody>
</table>
Spoofing – falsification of transmitted information
False Source – creates signal that is seen as coming from an incorrect location
False Content – content within messages are altered

Flooding – floods ARTCC radar screen with ghost airplanes
**False Alarm:** In this attack an adversary deliberately injects incorrect settings into the aircraft configuration system software. This tampering can cause the aircraft configuration to appear faulty therefore leading to unauthorized flight delays. This is ranked as medium.

**Aircraft Target Ghost Inject:** This attack is similar to the Ground Station Target Ghost Inject, except that the goal of the adversary is to inject “phantom aircraft” into the aircraft cockpit display. This is ranked medium to high.

**Ground Station Multiple Ghost Inject:** By executing this attack an adversary can replace the original parameters of an ADS-B signal and insert malicious strings, designed to attack a ground station.
Transmitter Aircraft

Aircraft Sensors (GPS)
Aircraft Transmitter
Aircraft Nav. Systems (FMS)

Receiver Aircraft

Aircraft Sensors (GPS)
Aircraft Nav. Systems (FMS)

Data Propagation

ADS-B Messages
ADS-B Receiver
Conflict Detection
Cockpit Display of Traffic Information
Flight Crew

Ground Station

ATCo
ATC Display
ATC Processing System
ADS-B Receiver
Traffic Messages
Traffic Broadcast
ADS-B Replay Attack

REPLAY ATTACK

Message injection

AND

Capture traffic

Write the Software to capture ADS-B out messages

Aircraft reconnaissance

Place transmitter in the correct position to ground station

Set up attack equipment

Set up required hardware

Set up required software

Write the Software to inject a ghost aircraft

AND

Adjust the required bandwidth
Target: Ground segment and air-ground segment. 
Attack Technique: Message injection and interception of ADS-B OUT.

Technical Difficulty: Medium. The attacker has to perform additional steps for the message injection. The attacker must intercept and capture the data and finally to replay the captured messages making use of message injection.

Impact: 4
ADS-B Replay Attack

- Capture ADS-B data:
  - UHD-mode
  - `uhd_rx_cfile.py --spec B:0 --gain 25 --samp-rate 4000000
    -f 10900000000 -v ~/CAPTURE_adsb.fc32`

- Pre-UHD-mode
- `usrp_rx_cfile.py`
- Replay the captured data:
  - UHD-mode
  - `tx_transmit_samples --file ~/CAPTURE_adsb.fc32 --ant "TX/RX" --rate 4000000 --freq 10900000000 --type float --
    subdev B:0`
  - Pre-UHD-mode, `usrp_replay_file.py`
Exploitation of ADS-B Vulnerabilities

Interception of ADS-B OUT

The technique is called as aircraft reconnaissance or simply eavesdropping.

Message Injection

This technique takes advantage of the ease to exploit the lack of authentication of the system.
Exploitation of ADS-B Vulnerabilities

Jamming
The execution of jamming disables one of various nodes in the wireless network from sending or receiving messages with enough power to disrupt 1090MHz frequency

Message Deletion
This attack is executed mainly by means of interference to delete messages from the wireless network
Exploitation of ADS-B Vulnerabilities

Message Modification

The integrity of the message is affected with the modification of the information contained in the message. The technique might be performed by two means, overshadowing and bit-flipping.
ADS-B?
What can happen when ADS-B sabotaged
How does ADS-B look like?

Community view

- ADS-B Out
  978 Mhz - Air to Air

- 30 Miles

- 7,000 ft

- Mode C

- You
  ADS-B Out

- Mode C
Encourage aviation to work together on the discovery, research and mitigation of cyber threats.

ADS-B require real security in-place in order to operate safely and according to the requirements.

Building information and assistance sharing channels (CERT).
Thank You!

Cyber Israel

Tom Alexandrovich
Aviation Guidance Manager
Critical Infrastructures Division

TomA@cyber.gov.il