ATN/IPPS Security Approach: two-way mutual authentication, data integrity, and privacy

Madhu Niraula, Jonathan Graefe, Ron Dlouhy Mark Layton, Mark Stevenson
Main Topics

- Safety Services and Messages or applications
- IPS architecture
- IPS architecture Considerations
- IPS Gateway
- Message Path and Security Considerations of the IPS traffic
- High-level flows with DTLS - Propose Security provision
- Securing the AVLC Layer for IPS
- AVLC+MIC Message details
- Key management
- Summary
- Q&A
IPS Background

• The aviation industry has recognized the limitations of current communications using ACARS and ATN
  • Aviation custom protocols, not IP compatible
  • Technical implementation issues of ATN in Europe
  • Security concerns
• To address these concerns the industry is moving to using the Internet Protocol Suite (IPS) for aviation communications
  • Framework in ICAO Doc. 9896
  • IPS utilizes modern internet protocol standards (IPv6) and COTS solutions
  • Compatible with future IP based subnetworks
  • Security provisions
• ICAO Doc. 9896 defines IPS while work on IPS standards is in progress in a number of aviation committees:
  • AEEC IPS subcommittee
  • RTCA SC-223
  • EUROCAE WG-108
  • ICAO Working Group I
• IPS implementation will support legacy (ACARS, ATN) aircraft and grounds systems during an extended transition to all IPS
ATS, AOC and ATC and Native IP applications Systems

- IPS supports ATC (FANS1/A, B1, B2) and AOC over AOA or ATN/OSI (Baseline 1 [Link2000+]), Baseline 2)
- ATN OSI, only B1 is being deployed (Based on FAA Roadmap B2 will not be deployed over ATN/OSI only over IPS)
Current Message Transfer Path

- FMS and other Aircraft Safety Critical System
- ATC and ATS applications Systems
- AOC Applications Systems

- Radios
- ACARS ATN OSI Message Router

- Enhanced GSIF w/ AOA, ATN, and IPS
- 0x8E IPI for IPS (AOA, 8208 ATN OSI)

- OSI Msg Processor
- BIS
- MATIP

- ATN OSI Legacy
- AOC and FANS 1/A legacy

- ACARS MSG Processor
- A620 Host

- AVLC XID, CMD and Info Frame

Aircraft

Ground
Message Transfer Process with ATN/IPS

ATN/IPS will use AVLC UI frame only

Aircraft

Ground

Enhanced GSIF w/ AOA, ATN, and IPS

0x8E IPI for IPS
(AOA, 8208 ATN OSI)

Radio

GS

GS RTR

RTR

ATN/OSI Legacy

AOC and FANS 1/A legacy

ACARS MSG Processor

MATIP

ACARS

ATN OSI

BIS

ATN IPS

ATN OSI

A623, AOC, FANS 1/A application Systems

B1, B2

A620 Host

IP ES

Enhanced GSIF w/ AOA, ATN, and IPS

ATN/IPS will use AVLC UI frame only

AVLC XID, CMD and Info Frame

AVLC UI Frame

8028 ATN AVLC Handoff

AOA

OSI Gateway

ACARS

GS CPU

GS RTR

RTR

GS CPU
## Service Port Definition

<table>
<thead>
<tr>
<th>Application</th>
<th>Port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication/Management</td>
<td>5908</td>
<td>Includes IP lookup and encrypted communication</td>
</tr>
<tr>
<td>(ATN) CM</td>
<td>5910</td>
<td></td>
</tr>
<tr>
<td>(ATN) CPDLC</td>
<td>5911</td>
<td></td>
</tr>
<tr>
<td>(ATN) ADS-C</td>
<td>5913</td>
<td></td>
</tr>
<tr>
<td>AOC</td>
<td>5914</td>
<td></td>
</tr>
<tr>
<td>(FANS) AFN</td>
<td>5915</td>
<td></td>
</tr>
<tr>
<td>(FANS) CPDLC</td>
<td>5916</td>
<td></td>
</tr>
<tr>
<td>(FANS) ADS-C</td>
<td>5917</td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>Other</td>
<td>Native IP Applications</td>
</tr>
</tbody>
</table>
Multiple IPS Attack paths

- **Assets**
  - Hackers
  - Attack Path

- **Aircraft**
  - Enhanced GSIF w/ AOA, ATN, and IPS
  - Radio
  - GS
  - GS RTR
  - RTR

- **Ground**
  - 0x8E IPI for IPS (AOA, 8208 ATN OSI)

- **AVLC UI Frame**
  - AVLC XID, CMD and Info Frame

- **AOC and FANS 1/A Legacy**
  - A623, AOC, FANS 1/A application Systems
  - B1, B2
  - ATN OSI
  - ACARS

- **ATN IPS**
  - IPS, ACARS, ATN/OSI Message Router
  - A429

- **IP ES**
  - ATN/OSI Legacy

- **ACARS MSG Processor**

- **MATIP**

- **BIS**

- **Manager**

- **Gateways**
  - 8028 ATN AVLC Handoff

- **Aircraft**

- **Ground**

- **Assets**

- **Hackers**

- **Attack Path**
Attack Paths

• Based on the specific aircraft architecture one or more attack paths can be exploited by adversaries with access subnetworks
  • The potential access subnetwork security related issues need to be resolved for IPS
  • Issue remains open for the ACARS and ATN/OSI
Securing the AVLC Layer for IPS

• Access network (VDL) Security
  • We propose using Datagram Transport Layer Security (RFC 6347 DTLS 1.2) over AVLC to ensure mutual authentication and data integrity. Allowing customers to choose to encrypt the data as per their wishes in accordance with the jurisdiction having authority.
  • Each message is protected with message integrity code (MIC) which is derived from the 32bits of SHA384 Message Authentication Code
  • DTLS is used to establish the MIC write keys that will be used to validate the message source and message integrity
  • Implement DTLS with mandatory replay attack detection and logging
  • It supports SCVP server interface for efficient certificate path discovery and validation
  • Make solution independent from CA provider
Securing the Message Gateway for IPS

• Access network Security
  • We propose using Datagram Transport Layer Security (RFC 6347 DTLS 1.2) over ATNPKT to ensure mutual authentication and data integrity. Allowing customers to choose to encrypt the data as per their wishes in accordance with the jurisdiction having authority.
  • Each message is protected with message integrity code (MIC) which is derived from the 32bits of SHA384 Message Authentication Code
  • DTLS is used to establish the MIC write keys that will be used to validate the message source and message integrity
  • Implement DTLS with mandatory replay attack detection and logging
  • It supports SCVP server interface for efficient certificate path discovery and validation
  • Make solution independent from CA provider
DTLS Provides

- Authentication of service provider to avionics
- Authentication of avionics to service provider
- Authentication independent of communications provider.
- Message Integrity Checks to verify the authenticity of messages
- Ability to allow higher layer encryption if desired
- Higher layer agnostic, ATN, ACARS, IPv6, UDP, TCP
- Peer reviewed via RFC process
IPS Security Provision

Security: Authentication & Integrity

FMS and other Aircraft Safety Critical System

A623, AOC, FANS 1/A application Systems

B1 or B2

ACARS MSG processor

ATN IPS

CMU/ATSU

ATN OSI

ATN/OSI Legacy

GS CPU

GS RTR

Enhanced GSIF w/ AOA, ATN, and IPS

Radio

GS

GS RTR

0x8E IPI for IPS (AOA, 8208 ATN OSI)

AVLC XID, CMD and Info Frame

AVLC UI Frame

8028 ATN AVLC Handoff

AOC and FANS 1/A legacy

A429

Radios

A620 Host

IP ES

ACARS

ATN OSI

Security

IPS Gateway

BIS

MATIP

FMS and other Aircraft Safety Critical System

A623, AOC, FANS 1/A application Systems

B1 or B2

ACARS

ATN OSI

Security

IPS Gateway

BIS

MATIP
Message Gateway - IP Dialogue Service Application Message Exchanges

IPv6

UDP

ATNPKT

Fixed Part

Variable Part

Application User Data

IPI

User Data

MIC

IPI = Initial Protocol Identifier, MIC = Message Integrity Code (Truncated 4 bytes of SHA-384)
AVLC message with MIC

AVLC UI Frame with segmentation support
- IPS only use UI frame
- For downlink Source AVLC address contains the aircraft address and Destination address contains the any valid ground address of the target DSP.
- Layer 2 segmentation protocol is added to support RFC 8200 minimum MTU limit of 1280 octets
- Sequence Number: Segment sequence number of this segment
- When message is not segmented, message number shall set to zero (0)
- Each segmented message contains a unique message number, when the message is segmented the message number indicates each segment that belongs to the specific message. Message number is incremented from 1 to 7 for the segmented message. The lowest available message number should be used for segmented messages.
- MIC is calculated and authenticated for each frame after the mutual authentication is done. For the DTLS handshake MIC is not included.
- MIC includes AVLC header as well as last octet of user data
- Retransmit timer at orange protocol layer is 3 seconds, up to 3 attempts only for fragmented messages (non message 0) based on high water mark ACK.
- If no acks are received at Layer 2 then retransmission will be handled by upper layer(s)
AVLC ACK message with MIC

AVLC UI Frame with segment Ack
  - IPI = 0x8E
  - ACK bit is set to 1
  - Sequence number: Next expected segment (note if there is multiple segment and missed the first segment, sequence number is set to 0). ACKs are high water mark based
  - Message number (RX_MSGN) this segment is ACKed for
  - Ack is only sent for the segmented message (not message number 0)
  - MIC cover AVLC UI frame header to the Message number
  - For authentication DTLS handshake, MIC is not included
VDL2 Link layer segmentation for IPS

The IPv6 packet (1280 bytes max) will be segmented as needed for VDL

The number of segments generated will depend on the size of the IPv6 packet and the maximum AVLC frame size (270 for IMS)

Each segments will be in a AVLC frame with the IPS IPI, the 'orange' protocol header and a MIC.

270 bytes max (when data is segmented, multiple segments sent in AVLC frame)

When the IPv6 packet is small, it will be contained in a single AVLC frame

270 bytes max (when data is not segmented)
Authentication / Key Management

- ECDSA keys pairs will be provided by the primary service provider for each aircraft subscribed.
- Keys will be signed by the primary service provider’s own or designate’s certificate authority (CA) key and be verifiable by any entity possessing the service provider’s or designate’s public key.
- Each aircraft will receive a public key and a private key. The public key is used for authentication with the IPS Gateway(s) and the private key is kept secret with the aircraft.
- To minimize the size of the public keys, suggest encoding in X.509 certificate DER format. The private keys are never transmitted.
- Each service provider or designate will maintain a service key directory of X.509 certificates for all aircraft for which they are the primary service provider. Each primary service provider to maintain a valid public CA X.509 certificate in DER encoding with all other trusted companion service providers for which a trusted relationship is established.
- Any key generated by the primary service provider that is later compromised, other than by expiration shall be listed in a certificate revocation list until the certificate expires. This list is to be shared no less than daily with all trusted companion service providers, even if no changes are recorded.
Result and summary

- Initial proto-typing: validation is being done using Openssl on the ground side and unoptimized version of RC DTLS and crypto library on the aircraft
- For the VDL< AVLC UI frame is being used
- Using the Root CA cert, one intermediate CA and server and aircraft Cert.
Q & A