

Security Convergence

Where IT meets the Airplane

Presenter: Patrick Patterson
President, Carillon Information Security Inc.

In the Beginning

- Analog was king
- Aircraft components were:
 - Simple
 - Single Purpose
 - Pure Hardware
 - Robust



Now

- “Glass Cockpit” means IT systems cross to the aircraft
 - Maintenance systems
 - Flight Software
 - Electronic Flight Bags



Classic Business IT is moving onto the Aircraft

- “The Aircraft is just another node on the airline network”
- And with it, comes the security concerns
 - Denial of Service
 - Impersonation
 - Malicious code
 - Virus
 - Trojan

```
STOP: 0x00000079 (0x00000002, 0x00000001,
0x00000002, 0x00000000)

Mismatched kernel and HAL9000 image.

Beginning dump of physical memory
Physical memory dump complete.
Contact your system administrator or technical
support group.
```

Communications

- VHF Voice being replaced by:
 - Voice over IP
 - more messages over ACARS
- Soon we will get to analog communications only for emergencies
 - Good: More traffic bandwidth available so more aircraft can move around safely
 - Bad: Network complexity increases and opens the door to attacks:
 - Spoofing
 - Denial of Service

Maintenance

- Hardware components replaced only during maintenance
- Software parts loaded “over the air” while aircraft is still in operation, replaced during turnaround
- Aircraft telemetry available in real time
- Good:
 - Shorter turn around times
 - Less aircraft “down” time
- Bad:
 - Source of software being loaded becomes critical
 - Confidentiality becomes important

Flight Ops

- Paper documents → electronic databases
- EFB's are laptops running Windows and Linux
- Gatelink is 802.11 “WiFi”
- Good:
 - Allows greater Airline efficiency (less costs)
 - More timely and accurate data for Pilots and maintenance
 - Cheaper to implement
- Bad:
 - Much easier to “spoof” an electronic document or communication path

Passenger Applications

- In Flight Entertainment
- Duty Free Credit Card Purchasing
- Passenger Internet and Cellular
- Good:
 - Better Passenger experience
 - Revenue opportunities for airline
- Bad:
 - Network segregation is critical
 - Passengers don't have a way to know what is “safe”

Proprietary vs. Open

- Proprietary Air Communications data and voice protocols replaced by IP Networks that may be tied to other, non-aircraft networks.
- Good:
 - Brings less cost and complexity
 - Opens new avenues for service provider competition
- Bad:
 - The bar is lowered for “the bad guys” to cause trouble.

Identity becomes critical

- Most of the attacks are identity based:



When Identity is not sure

- Air Traffic Control could have a bad day
 - Transponders work by “honour system”
 - ADS-B must be designed with unforgeable identity
- Airline could get billed for other's use of networks
 - ACARS Traffic
 - Passenger Internet and Cellular

ATA DSWG Solutions

- New Spec 42:
 - Risk Mitigation framework
 - PKI Guidance
 - More to come soon
 - Please join us to help us address your security concerns!

Risk Mitigation Framework

- Based on ARINC Report 811
- Best Practice for evaluating:
 - Communication path risks
 - Implementation risks
- Mainly for solution providers
 - Operators could use as well.

Public Key Infrastructure

- Industry direction for Identity Management
 - Aircraft Identity
 - Personnel Identity
 - Device (Servers, etc.) Identity
 - Corporate Identity
- Required on 787 and A380
 - Gatelink
 - Software Data Loading
 - ACARS Message Security
 - Maintenance uplink to aircraft
 - Electronic Flight Bag applications

Public Key Infrastructure

- Direction for future services
- Anything today that requires a physical signature is moving to electronic form
 - 8130 / Form 1
 - Log Books
- Enabling base technology for “extended enterprise”
 - Federated Identity Management

Public Key Infrastructure

- CertiPath and other industry “Bridges” help make managing identity easier
 - Single Trust partner to manage
- DSWG approach ensures Identity Security
 - Mitigates spoofing, reduces cost through:
 - Allowing adoption of new services outlined
 - Risk Reduction of misidentification
 - But only when fully implemented
 - Implementors should aim for cross-certification with a bridge
 - Definitely have implementation audited

Change impacts

- Suppliers
 - Maps
 - Flight and Passenger applications
 - Fuel
 - Cargo
 - Catering

Change Impacts (cont)

- Government agencies
 - Weather Office
 - National Regulatory body for flight plans
 - Air Traffic Control
 - Customs

Change Impacts (cont)

- Other Airline departments off of the airplane
 - Maintenance
 - Ground crew
 - Flight Operations

Questions?

Contacting me

Patrick Patterson

ppatterson@carillon.ca

+1 514 485 0789

<http://www.carillon.ca>

Next DSWG Meeting

Montreal, Quebec, CANADA

Week of November 10th