FAA Security

State of the State and Beyond

Presented to: 2008 National Software and Airborne Electronic Hardware Standardization Conference

Written by: Kevin Harnett and Vince Rakauskas (DOT/Volpe Center)

Presented by: Ray Decerchio (FAA/AIR-120) and Vince Rakauskas (Volpe)

Date: August 20, 2008
Agenda

• Airborne Network (AN) Cyber Security Issues

• Key Topics & Challenges

• What is being done now?
  • Aircraft Issues
  • Infrastructure Issues
Airborne Network (AN)
Cyber Security Issues

----

Aircraft & Infrastructure
Aircraft Data Network (ADN) Domain Concept

- **Aircraft control**
  - Flight and Embedded Control Systems
  - Cabin Core
  - Control the Airplane
  - Closed

- **Airline Information Services**
  - Admin
  - Passenger Support
  - Operate the Airline
  - Private

- **Passenger Information and Entertainment Services**
  - Entertain the Passengers
  - Public

- **Passenger-Owned Devices**

Airborne Cyber Security Issues

Airlines will use Broadband Internet connectivity to support passenger services then use existing bandwidth to support operations.

Revenue from passenger services provides funding for increased infrastructure costs.

New vulnerabilities are added

Technology Advances enable new, cost-effective connectivity between on-board Networks and Airline Ground Networks

Vulnerabilities

- Aircraft Control
- Cabin Services
- ADN
- IFE
- Crew Devices
- Internal 802.11
- External 802.11
- Psgr Devices
- VHF/HF
- SATCOM
- Broadband
Airborne Cyber Security Issues

Mission-critical systems are potentially susceptible to attack
Airborne Cyber Security Issues

These cyber security vulnerabilities are not only new but have not been anticipated.

Since it has not been a concern in the past, the existing Code of Federal Regulations does not specifically address cyber security vulnerabilities.

Consequently, there are no existing Policies, Certification Criteria or Procedures that provide assurances that cyber security vulnerabilities will not cause unsafe flight conditions.

Cyber security vulnerabilities in the ADN will be irrevocably bound to the safety of flight.

Unmitigated, these vulnerabilities will have a definite negative effect on the safety of flight.
Airborne Cyber Security Issues

There are cyber security issues that extend well beyond the aircraft itself.

The following graphic will present an over-simplified depiction.
Airborne Cyber Security Issues

Commercial & Military

Emerging NAS Systems (i.e. ADS-B)

NextGen

Commercial Ground Systems (IFE – Internet)

DoD (GIG)

Domestic & Foreign

Net Centric

Airline Operations Centers

SWIM

Vulnerabilities

Assurances

NAS Systems (i.e. ADS-B)
Airborne Cyber Security Issues

“Groundworthiness” – Assurances that communication with aircraft do not negatively impact airworthiness

Technical Issues

- Identification and authentication
- Trust
- PKI/Key Management
- Boundary and Perimeter Defenses
- Net-Centric Security Mechanisms
- Auditing, IDS and Incident Response
- And so on…

FAA Assurances - Certification Criteria

Maintain assurances
Key Topics and Challenges
Key Topics & Challenges
Aircraft

- Documented Cyber Security Certification Criteria and Processes that are acceptable to FAA are not yet written

- Issues are abundant, non-trivial and unresolved

- Safety vs. Security Paradigm
Key Topics & Challenges

Infrastructure

• Many programs currently developing Concepts of Operations and Security Architectures
• Coordination of NextGen/FAA, DoD and Aviation Industry on security architectures and information sharing
• It will require focused collaborative effort to resolve these issues
  • Global naming/addressing
  • Global trust paradigm

NextGen = Next Generation Air Transportation System
Key Topics Requiring Focus & Resolution

Key Programs are not coordinated and do not have harmonized goals

Don’t get so focused on the task at hand…
That you lose awareness of what’s going on around you
Key Topics & Challenges
Maintaining Assurances

• It will be a challenge to maintain flight safety assurances in a dynamic and changing environment
• Procedures for maintenance will also need to be developed
• Airborne Cyber Security Training will be critical
• Planning needs to begin now
What is being done now?

Aircraft Security Issues
Key Current Activities
Aircraft

• RTCA SC-216 Aeronautical Systems Security
• FAA Software and Digital Systems (SDS) Airborne Security Requirements to Ensure Aircraft Safety
• Volpe Center Cyber Security Projects
• NIST Risk Management Framework (RMF) – to be covered in the EFB and Security briefing (Peter Skaves, FAA)
Key Aviation Industry Programs

- EUROCAE's WG-72, Aeronautical System Security Working Group
  - Module 1 – Airworthiness
  - Module 4 - Security Control, Operation and Management
  - Module 5 – Air Transportation System Security Reference Model
- ARINC Network Infrastructure and Security (NIS) Subcommittee and ARINC 811 Commercial Airlines Security CONOPs Paper
- ATA E-Biz's Digital Security Working Group (DSWG) and Certipath
RTCA SC-216
Aeronautical Systems Security

Designated Federal Official (DFO): Ray Decerchio
RTCA SC-216 Aeronautical Systems Security

Requirements Assessment
The Special Committee is needed to bring together aircraft manufacturers and systems designers, CNS/ATM systems designers and operators, airlines maintenance and operations personnel and government (primarily DHS/TSA, FAA, DoD) to form a consensus and document guidance for a network security assurance process and acceptable means of compliance for safe, secure and efficient airspace operations.
RTCA SC-216 Aeronautical Systems Security

RTCA SC-216 Deliverables – December, 2009

• Minimum Aviation System Performance Standards (MASPS) for Aeronautical Electronic and Networked Systems Security
• Security Assurance and Assessment Processes (SAAPM) and Methods for Safety-related Aircraft Systems
RTCA SC-216 Aeronautical Systems Security

• MASPS objectives:
  Specify security information that should be useful to designers, manufacturers, installers and service providers for Aeronautical Electronic and Networked Systems. The MASPS will need to define the Security Domain Reference Model for the Air Transportation Systems (input provided by Eurocae WG-72, Module 1).

• MASPS will define guidelines for:
  • Selecting, operating, and managing security controls
  • Managing security concerns involving external systems and/or organizations
  • Design & architecture for compliance with the processes and methods (e.g. layered protection, crew alerting)
RTCA SC-216 Aeronautical Systems Security

• **SAAPM Objectives:**
  Propose guidance for systems affected by security considerations to be developed and assessed, such that compliance with FAR 25.1309 can be demonstrated. This document may draw on ARP 4754, DO-178B, DO-254, and other material in addition to the security standards below to develop an acceptable security assessment and assurance process that can be used to show compliance with airborne systems safety regulations.

• **SAAPM will develop guidance for:**
  • Process for ATS Groundworthiness security assessment and assurance
  • Process for aircraft certification for security assessment/assurance, security validation/verification, and airworthiness security certification
  • Methods for aircraft certification for security assessment/assurance and complex aircraft systems security analysis
  • Means of compliance in terms of criteria for applying methods and assurance regarding FAR 25.1309
FAA Software and Digital Systems (SDS) Security R&D Project
Phase 3: Airborne Security Requirements to Ensure Aircraft Safety
SDS Phase 1 & 2 Study Overview

In 2004, FAA commissioned two year study “LANS in Aircraft”

- Conducted by Boeing Phantom Works (December 2007)
- Document evaluation criteria that can be used by certification authorities and industry to ensure onboard LANs will not negatively impact aircraft safety
  1. Identify safety and security issues
  2. Determine how both safety and security can be addressed without compromising the other
  3. Develop acceptance criteria to address certification and safety concerns for use of LANs in aircraft
- Identified recommendations related to:
  1. DO-178B and APR-4754
  2. Integrity Models
  3. DoD processes and standards
  4. Testing adequacy
Software and Digital Systems (SDS) Program

- Prior Phase Reports
  - Networked Local Area Networks (LANs) in Aircraft: Safety, Security and Certification Issues, and Initial Acceptance Criteria (Phases 1 and 2)
  - Handbook for Networked Local Area Networks (LANs) in Aircraft

- Current Phase
  - Airborne Security Requirements to Ensure Aircraft Safety (Phase 3)
Software and Digital Systems (SDS) Program

Airborne Security Requirements to Ensure Aircraft Safety - Objectives

• Identify new technology and accesses to aircraft networks and systems
• Determine the potential security vulnerabilities to the aircraft
• Propose recommendations for security protection requirements for the aircraft and its systems
• Ensure these recommendations are consistent with current security requirements, including
  • Focus on aircraft safety
  • Department of Homeland Security (DHS)
  • Military
  • Communications, Navigation and Surveillance and Air Traffic Management (CNS/ATM)
  • Aircraft operators
Phase 3: Airborne Security Requirements to Ensure Aircraft Safety Research Task

Timeline:
- Dec 2006
- Feb 2008 – Feb 2009
- Mar 2009

Task 1: Reassess Phase 2 Finding and Recommendations
- Task 1.1: SDS Phase 2 Reassessment Report
- WP1: SC-216 SG2 Assessment and Recommended Methodology/Process
- WP2: SDS Phase 2 Reassessment WP for SC-216 (WP2)
- WP3: TBD

- WP5: UASs and Cyber Security

Task 3: Summary Draft and Final Phase 3 Report

Phase 4: TBD

Phase 1 SDS LAN Report
- SDS Phase 2 Final Report & Handbook

Phase 2 SDS LAN Report

Phase 3: Airborne Security Requirements to Ensure Aircraft Safety Research Task
NIST
Risk Management Framework
(RMF)
NIST RMF

• Follows Federal Information Security Management Act (FISMA)
• Establishes mandatory minimum IS standards and guidelines
• RMF promotes a disciplined, structured, and flexible process for applying the NIST security standards and guidelines
• NIST special publications (e.g. 800-53, 800-53A)
• Accepted by the FAA
• Other key critical infrastructures are “tailoring” NIST RMF (e.g. USAF/Defense Industrial Base, DoD/DHS/Intelligence, and Supervisory Control Data Acquisition Systems-SCADA)
Risk Management Framework

Starting Point
FIPS 199 / SP 800-60

SP 800-37 / SP 800-53A

Monitor Security Controls
Continuously track changes to the information system that may affect security controls and reassess control effectiveness

SP 800-37

Authorize Information System
Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-53A

Assess Security Controls
Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-60

Categorize Information System
Define criticality/sensitivity of information system according to potential impact of loss

SP 800-70

Implement Security Controls
Implement security controls; apply security configuration settings

SP 800-18

Document Security Controls
Document in the security plan, the security requirements for the information system and the security controls planned or in place

Select Security Controls
Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

SP 800-53 / SP 800-30

Supplement Security Controls
Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-53 / SP 800-53

Select Security Controls
Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

FIPS 200 / SP 800-53

Allocate Security Controls
Allocate security control requirements to individuals and/or systems to protect the information system

FIPS 199 / SP 800-60

Monitor Security Controls
Continuously track changes to the information system that may affect security controls and reassess control effectiveness
Vision – The way Forward

Aviation Industry Programs

Government Programs

Push

This goal will be significantly more difficult to achieve than it appears in this simple illustration

Pull

Aviation Industry Programs toward NIST RMF

NIST RMF

Pull

Government Programs toward NIST RMF

NIST RMF
What is being done now?

Infrastructure Security Issues
Key FAA Programs

- Joint Planning and Development Office (JPDO):
  - Net-Centric Operations (NCO) and Aircraft/Avionics Working Groups

- ATO-P NextGen Enterprise and Security Architecture

- System-Wide Information Management (SWIM) Security Architecture
Volpe Center Airborne Network IA – Related Projects

- Air Force and UK Center for Protection of National Infrastructure (CPNI) Collaboration on Security Use Cases and Attack Scenarios
  - Electronic Flight Bags (EFB)
  - Flight Object (FO)
  - Automatic Dependent Surveillance - Broadcast (ADS-B)
  - Others

- FAA Safety and Digital System (SDS) Airborne Security Requirements to Ensure Aircraft Safety Research (& FAA SC-216 Support)

- FAA NextGen Security Architecture Support

- FAA Boeing 787 & Future Aircraft R&D Cyber Security Assurance Support

- FAA Aircraft Certification Cyber Security Assurance Training (TAD Specialists)

- FAA RTCA SC-216 (Aeronautical System Security) Support
Issues For You To Consider

• Everybody doing the right thing = Safe Flight
• What role will you play in providing the cyber assurances that will insure safe flight?
• How will your job responsibilities change?
• Will there be a need for new security positions?
• Will your responsibilities be supported by emerging rules?
• Do you have the necessary skills to accomplish new responsibilities?
• What training will you require?
One Potential Solution
Thank you

We are Cyber Security Professionals
And
Committed to Your Success

Any Questions???
Contact Information

Raymond Decerchio, RTCA SC-216 DFO, AIR-120 FAA
   Email: Raymond.W.Decerchio@faa.gov
   Phone: 202-267-3095

Kevin Harnett, Volpe Center Cyber Security Program Manager
   Email: harnett@volpe.dot.gov
   Phone: 617-699-7086

Vince Rakauskas, Security Engineer
   Email: rakauskas@comcast.net
   Phone: 508-339-0280
Backups
Summary

Major and serious security threats by organized security hacker groups in Nation States (like China)

- Impact to next-generation commercial aircraft and A/G communications due to open and COTS systems (e.g. B-787, A-380, A-350)
- Related links:
  - US warned of 'aggressive' Chinese cyberspying
  - Chinese cyber strikes will be 'like WMD'
  - 2007 REPORT TO CONGRESS of the U.S.-China economic and security review commission

Current problem of “no” regulatory guidance needs to be resolved before the next set of next-generation aircraft (i.e. A-350 XWB, Boeing Y-1, UAV/UAS, others) are deployed

For NextGen to be successful… the issues (i.e. updated regulations, security tools) regarding security airworthiness and certification needs to be resolved !!!
Joint USAF/Civil AN Cyber Security Study

Security Certification Criteria and Post-Maintenance Assurances
- C1 - Potential Viability of Joint FAA/DoD Certification Criteria
- C2 - Identification of Certification Toolsets
- C3 - Maintenance & Post-Maintenance Assurances

Secure Mechanisms
- SM1 - Collaborated Technical Security Mechanism Solutions
- SM2 - Standardization of Technical Solutions
- SM3 - Ground Entry Point Characterization and Vulnerability Assessment
- SM4 - User Identification & Authentication

IDS, Auditing, and Continued Operations
- IDS1 - Auditing, IPS/IDS & SIM toolsets
- IDS2 - Auditing, IPS/IDS, SIM & Incident Response CONOPS
- IDS3 - Specifications for Continued Operations
Airborne Cyber Security Issues

- NextGen – SWIM - NewNAS
- Aviation Industry Standards
- Aviation Industry Manufacturers - Proprietary Solutions
- FAA Special Conditions
- Commercial Architecture
- Military Architecture
- Commercial Derivative Aircraft Issues
- Airborne Network
- GIG
- Joint Airborne Network Service Suite (JANSS)
- Airborne and Ground Information-Operations System (AGIS)
SWIM Operational Concept
Primary differences:
1. Aircraft Control, and Airline Information Services share a common network system.
2. Specific Aircraft Control and Airline Information Services processes form distributed network relationships with NAS ground computers by using an IP-based air-to-ground link.

The air gap between the aircraft passengers and the avionics systems remains intact.
This Phase 1 slide does not show how the VPN encapsulation (and decapsulation) is accomplished.
Volpe Center Projects

Focused on a cyber security solution that will support FAA/USAF requirements
Otherwise unbiased
Catalyst for Collaboration
Resolution of uncoordinated goals
Joint USAF/Civil AN Security Study - Gaps

Security Certification Criteria and Post-Maintenance Assurances

C1 - Potential Viability of Joint FAA/DoD Certification Criteria
Correlation of aviation industry security certification standards (e.g. DO178B, CC, FISMA) and AN requirements for CDA (e.g. DoD 8200.2, GIG, AN)

C2 - Identification of Certification Toolsets
Identification of needed tools to support certification – IA Tool Sets for IP-based and non-IP based airborne LANs including penetration test, code/malware checkers, etc.

C3 - Maintenance & Post-Maintenance Assurances
Maintenance procedures and tool sets that will insure authorized changes (patch mgt, VA compliance validation, anti-virus updates, security configuration, etc) and post-maintenance procedures and tool sets to insure against invalidation of the certification due to maintenance changes including definition of condition requiring recertification
Secure Mechanisms

SM1 - Collaborated Technical Security Mechanism Solutions

CDA will need to resolve the same issues that are outstanding on the AN IA issues list but are being designed outside the context of the GIG/AN enclave. Collaboration needs to be done that has an objective of compatible if not matching technical solution on the following IA issues:

- Definition of security boundaries
- Secure Air/Ground Communications
- Routing Protocol Security mechanisms
- Performance Evaluation
- IPv6 - timetable for AN versus commercial ADN
- IA Service/Function Automation
- IA Support Services
Secure Mechanisms (cont.)

SM2 - Standardization of Technical Solutions
Standards and design consideration for CDA are being decided in projects that are not fully coordinated. Coordination of the following efforts will be needed to provide the best IA solution for CDA.

SM3 - Ground Entry Point Characterization and Vulnerability Assessment
There is a lack of a concerted effort to fully characterize Ground Entry Points (GEP) and perform a GEP vulnerability assessment. This needs to be accomplished to insure secure Air-Ground Data Communication Links (ADS-B, CPDLC).

SM4 - User Identification & Authorization
Due to a cultural resistance in the aviation industry there a lack of effort being conducted on Identification and Authorization of users.
IDS, Auditing, and Continued Operations

IDS1 - Auditing, IPS/IDS & SIM toolsets
There is a need to resolve open issues regarding the selection and implementation of toolsets to support auditing, intrusion prevention/detection, and Security Information Management (SIM)

IDS2 - Auditing, IPS/IDS, SIM & Incident Response CONOPS
There is currently a lack of the necessary level of work and involvement to create a CONOPS for Incident Response.

IDS3 - Specifications for Continued Operations
There appears to be a lack of the necessary level of work and involvement to determine the requirements and technical solution to provide for continued operation in the event of a successful cyber attack on aircraft and aircraft support systems that will support the next generation of aircraft.
Key Government Programs

DoD Airborne Network (AN) Platforms
USAF Airborne Network (AN) Information Assurance (IA) Program
USAF Multi-level Independent Level Security (MILS)/Multi-Level Security (MLS)
DHS Security Programs (e.g. DHS/DoD Software Assurance Forum and Software Assurance Metrics and Tool Evaluation (SAMTE), US CERT FX Software Forum, and HSARPA Cyber Security R&D Program)
UK Ministry of Defense (MoD) Safety/Security (SafSec) Initiative
RTCA SC-216 Aeronautical Systems Security

Problem Statement
Existing aircraft system safety guidance does not specifically address airborne network and data security issues
Non-standardized and potentially inequitable agreements between the various applicants and the various regulatory agencies on an acceptable process and means of compliance for ensuring safe, secure and efficient aircraft network design and operations
Existing information technology (ground-based systems) network and data security assurance processes are not easily adapted to the aviation system environment and do not address aspects of ATM/CNS ground-based and aircraft systems.