



The National Transportation Systems Center

Initiation and Maintenance Electronic Security Procedures for E-enabled Aircraft

Presented to: ICNS 2009

**Written by: Kevin Harnett and
Chris Riley (DOT/Volpe Center)**

**Presented by: Chris Riley
(DOT/Volpe)**

Date: May 2009

**This work was supported by the FAA
Research and Technology
Development Office, Airport & Aircraft
Safety Group, Flight Safety Team,
Atlantic City Int'l Airport, New Jersey**

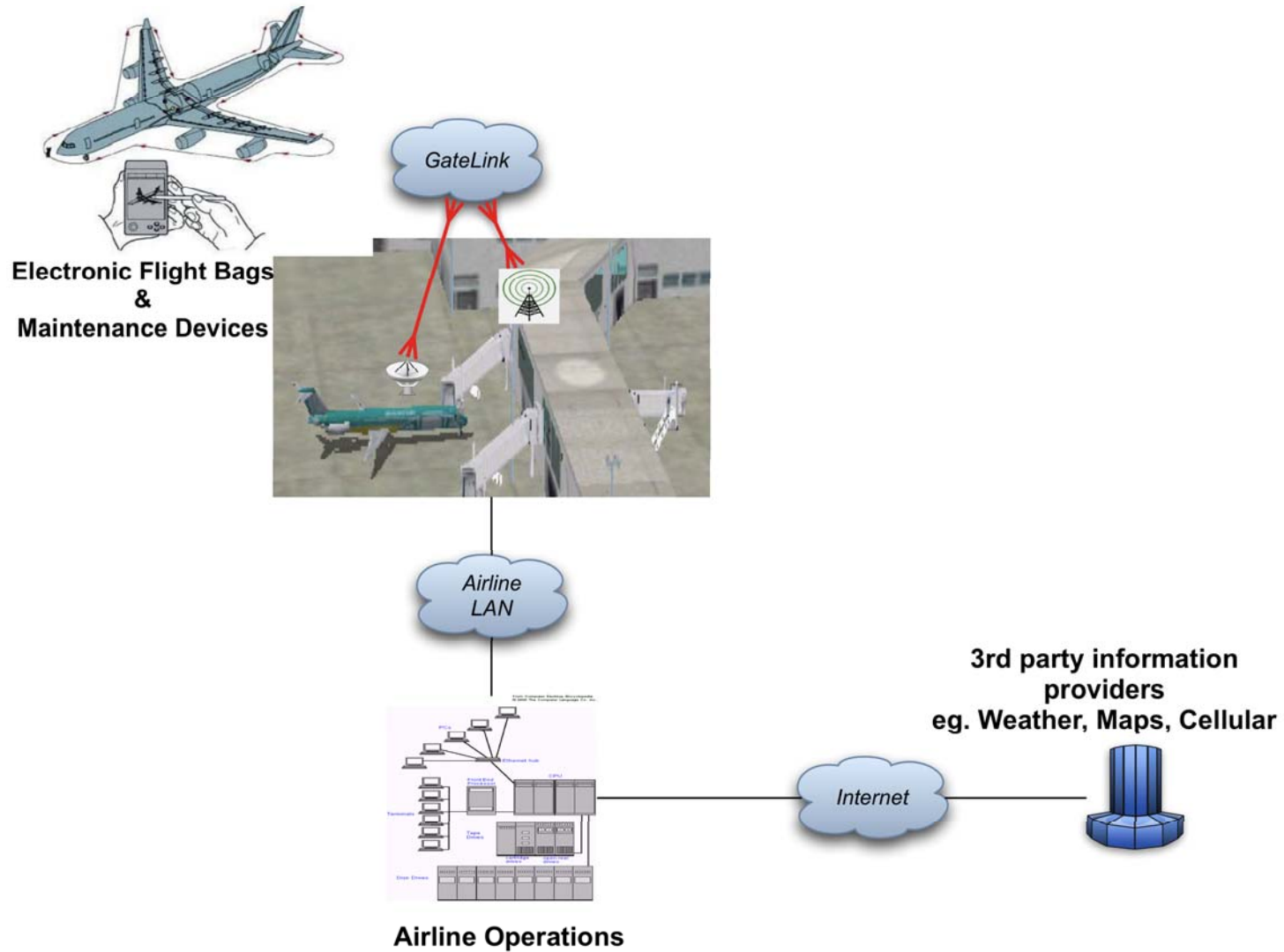


**U.S. Department of Transportation
Research and Innovative Technology Administration**

Overview & Process

- Review applicable guidance material from RTCA, ARINC and Eurocae
- Develop a security control questionnaire based on NIST 800-53 tailored for this environment
- Interview
 - Airplane Manufacturers (Boeing, Airbus)
 - Operators (Northwest, United, Continental, SITA)
 - Flight Standards (AFS-300)
- Participate in industry working groups (RTCA SC-216, Eurocae WG-72)
- Summarize findings from all sources

Operational Environment



General Findings

Integration and standardization

- Limited network bandwidth
- Mobility of the aircraft
- Must communicate/trust a large number of partners.
- Disconnects in interoperability break the trust chain

Cost driven design –

- Manufactures and operators focus on reduced cost given the current lack of guidance for security compliance.
- Security features do not generate revenue while robust implementations are expensive
- Tendency to implement solutions solving immediate problems.
- Given an adequate picture of the regulatory environment, robust implementations would produce cost savings.

Technology & Training Issues

Interoperable Approach To Digital Certificates And Public Key Infrastructure

- Digital certificates and *PKI* are used extensively to protect the confidentiality and integrity in this environment as such the protection of the encryption keys is critical.
 - Software Loadable Parts, EFB , Gatelink connection, maintenance laptops, software configurations all rely on digital certificates
- Key protection includes; distribution, storing, access and aging
- Terrestrial networks typically use a centralized approach to manage and revoke keys
- Low network bandwidth in the airborne network environment, require special considerations for the distribution and key management
- Unique requirements prohibit an industry adoption of a standards based approach
- Research in this area of a common trust model, cross certification and common root certification authority could be used to identify unique approaches in providing confidentiality and integrity controls considering the challenges of this environment.

Technology & Training Issues

Log Standardization To Promote Threat Identification And Response

- No industry standard defining the type of information and format for security audit logs
- Log standardization insures adequate information is collected while standard format promotes centralized management and visibility of security posture
- Mitre's Common Event Expression (CEE) are attacking this problem but are still in their infancy.
-
- Airborne networks have different requirements and constraints so there is no guarantee that CEE solution will be applicable without active participation.
- Research should identify the type of information, format and timeliness required by this environment while participating in standards activities like CEE to move toward a centralized approach.

Technology & Training Issues

Compliance Programs And Training Framework

- Airborne network standard bodies currently focus on providing a unified approach to implementation and management.
- Different skill sets will be required, to operate and regulate this environment, there has been no definition of what those skill sets are.
- Manufacturers develop specific training packages supporting their individual products however; no standardization across products or manufacturers should be expected.
- Research is needed to identify critical training areas and tools required for operations and regulation of this security environment
- Develop a framework identifying key training areas along with evaluation criteria.

Summary of Findings

Environment: Aircraft Manufacturer

Finding Area	Recommended FAA Research Project Summary
Trusted communication paths between airplane and gate	Participate in ARINC NIS committee and contributed research to promote identity federation of users and devices in this environment.
Digital Key Management	Research digital certificate providers and federated interoperability capability being developed in cross certified federal bridge programs.
Audit log standards	Participate in Mitre's Common Event and Expression (CEE) to define log standardization for the airborne network environment.

Summary of Findings

Environment: Airline Operations

Finding Area	Recommended FAA Research Project Summary
Limited Communication Bandwidth	Research alternative strategies specific to an aircraft network environment.
Secure remote communication	Research security risks associated with communications solutions currently provided by manufacturers and operators.
Digital Certificates and PKI	Research common trust model, cross certification and common root certification authority to identify unique approaches in providing confidentiality and integrity controls considering the challenges of this environment.
Identity Management	FAA research and participation in standard groups such as OASIS to aid in the development of a federated identity approach.

Summary of Findings

Environment: FAA Flight Standards

Finding Area	Recommended FAA Research Project Summary
Regulatory Guidance on Airborne Network Security	Form a FAA task force to assess the organizational impact of increased workload, monitoring, information systems and workforce skill sets and training required
Tracking System and Job Aids For Regulators	Form a FAA/industry task force to determine the types and level of tools that regulators will require. Evaluate the feasibility of incorporating the functionality into ATOS
Security Compliance Program and Training	Perform FAA research in the areas of security compliance, minimum qualification of inspectors and a training framework to identify and prioritize specific needs while providing a mechanism to evaluate proficiency.

Questions & Comments