Challenges for IT Infrastructure Supporting Secure Network-Enabled Commercial Airplane Operations

Richard V. Robinson[1], Krishna Sampigethaya[1, 2], Mingyan Li[1], Scott Lintelman[1], Radha Poovendran[2], and David von Oheimb[3].

[1] *Boeing Phantom Works, Bellevue, WA 98008, USA*

[2] *Network Security Lab (NSL), University of Washington, Seattle, WA 98195, USA*

[3] *Siemens Corporate Technology, Germany*

[Abstract] The numerous benefits of enabling commercial airplanes to communicate over networks are only obtained at the price of introducing security threats to onboard systems. A primary threat arises from the opportunity for corruption of safety-critical and business-critical airplane loadable software distributed via networks from off-board systems. The FAA recognizes that the unprecedented use of such applications in network-enabled airplanes impacts well-established safety regulations and guidance. In this paper, we present a framework for securing airplane software distribution and overview the main challenges. For facilitating integration into existing certification guidelines for airplanes, we employ the Common Criteria standard based approach to security evaluation of IT infrastructure for airplane network applications. Additionally, we present some open problems in network-enabled airplane security.

I. Introduction

THE convergence of rapidly expanding world-wide data communication infrastructures, network-centric information processing, and commoditized lightweight computational hardware, has brought the aerospace industry to the threshold of a new era in aviation: the age of a fully network-enabled or "eEnabled" airplane. The prospects in commercial aviation are exceedingly optimistic for airline businesses and the flying public alike, as the eEnabled airplane promises to provide a basis for improvements in passenger amenities, schedule predictability, maintenance and operational efficiencies, flight safety, and other areas.

However, as large-scale airplanes employ more internal computer processing and network facilities, and become connected with network environments off-board, opportunities for information security attacks may open. The widespread use of commercial off-the-shelf components raises the potential for re-engineering and sabotaging aircraft IT components. Regulatory institutions have yet to systematically address information security needs appropriate to commercial aircraft, such as the network-enabled 787-8 airplane model.[10,11] Indeed, while the framework informing safety engineering principles and practices for airplanes and airplane software is mature and widely agreed (e.g. RTCA DO-178B), no such framework exists for corresponding information security needs.[4]

This paper describes an approach and methodology for addressing one specific, well-defined aspect of the eEnabled airplane security problem, viz., electronic distribution of airplane loadable software. Today, industry standard mechanisms for retaining and distributing airplane loadable software parts[1] are evolving away from processes that handle physical storage media, in favor of electronic storage and distribution via computer networks.[2] We analyze security issues that emerge when information networks are used to store and distribute airplane loadable software and describe an approach to ensuring the integrity of such parts throughout their lifecycles.

Correctness of certain airplane loadable software components, e.g. flight control computer software, has direct safety implications. This self-evident observation is addressed at length in the standards and advice mandated such as in Ref. 1, for assuring quality of airplane loadable software during its design and development. Therefore, the integrity of safety-critical software parts must be protected at all times. However, the use of public networks for storing and distributing airplane software may expose vulnerabilities that can be exploited for attacks on the integrity of parts, potentially posing a threat to airplane safety by reducing safety margins. Furthermore, attackers

might exploit vulnerabilities to compromise systems in a manner that reduces passenger comfort and confidence, impedes airline business processes, or creates unwarranted delays or expenses. In effect, the industry's investment in the safety and reliability of airplane software is at risk.

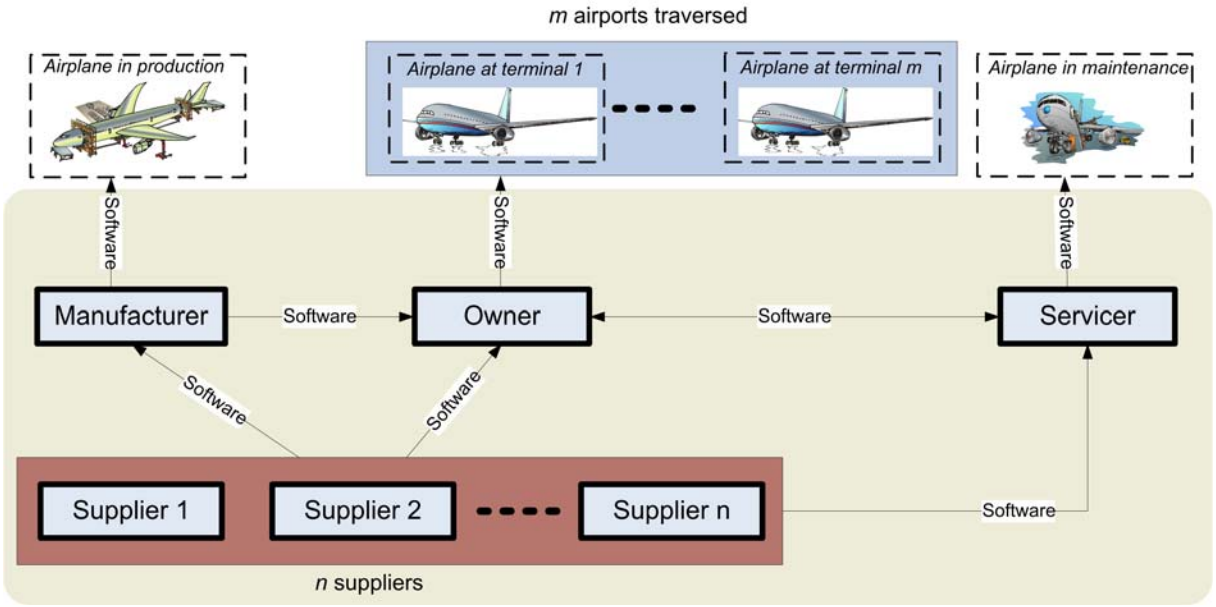

Figure 1. Illustration of the Airplane Asset Distribution System (AADS) model and its constraints, i.e. multiple suppliers delivering software to airplane, and multiple airports are traversed by airplane.

In this paper, we summarize our analysis of requirements for a generic heterogeneous system for electronic storage and distribution of airplane software (Airplane Asset Distribution System or AADS).[3] We identify the security threats, and propose countermeasures in the form of security primitives sufficient to address the threats comprehensively.

The rest of the paper is organized as follows. Section II presents the AADS model, security threats to AADS, and requirements for mitigating these threats. We also outline a solution approach based on digital signatures that can provide end-to-end security for AADS. Section III discusses various unprecedented challenges presented by the secure AADS to airplane operators. Section IV discusses open problems and future directions in the area of eEnabled airplane security, and Section V concludes this paper.

II. Securing the Airplane Asset Distribution System (AADS)

A. System Description

Fig. 1 shows the constituent entities in the AADS model. As illustrated in Fig. 1, upon safety-assured development of loadable software at the supplier, the software is distributed to an intermediate entity, i.e. the airplane manufacturer, owner (i.e. airline) or servicer. The intermediate entity stores and distributes the loadable software to the airplane. An attacker can attempt to corrupt software by exploiting network and system vulnerabilities or as an insider at an intermediate entity. Additionally, we consider the following constraints of the AADS system. As will be seen in Section III, these constraints can complicate the design of the secure AADS by requiring tradeoffs.

- (*C1*) Fig. 1 illustrates that an airplane can traverse multiple airports with different networking capabilities. Each airport where the airplane is to receive software may employ one among many available wireless standards for its network, or may not have any network connectivity altogether. Therefore apart from interoperability, an airplane is faced with *intermittent connectivity* along its traversed path. Moreover, at each traversed airport, the airplane may need to communicate with *multiple off-board* systems.
- (*C2*) Fig. 1 also shows that an airplane can receive software from *multiple suppliers*. Additionally, in the presence of multiple owners and servicers at each traversed airport, the airplane must accept software only from its owner and/or authorized servicer.

- (*C3*) As a business objective for the AADS, the impact of security requirements on the airplane owner must be reduced.
- (*C4*) Changes to the AADS (e.g. use of onboard networks and security mechanisms) with potential impact on airplane safety warrant modifications to mandated airplane safety regulations and guidance.

We assume that the airplane operator verifies the loadable software configuration to be correct after upload to onboard systems. The verification is enabled by an airplane configuration list of software parts available to the operator. We also assume the airplane loadable software design is fault-tolerant, e.g. multiple instances of software exist in system to prevent a single point of failure during execution. Nevertheless, threats to the AADS emerge as discussed next.

B. Security Threats

Data networks have vulnerabilities that can be exploited by attackers attempting to manipulate distributed software.

Airplane safety threats. For lowering safety margins of an airplane, attackers can attempt to manipulate that airplane's safety-critical software parts (e.g. DO-178B Level A parts) during distribution. A software part can be manipulated by either corrupting it or delaying the uplink of its latest version. Additionally, parts can be replayed, blocked or diverted to manipulate the airplane software configuration, such as by making it contain incorrect software parts or part versions.

Fortunately, safety threats can be mitigated to an extent. Any manipulated software may be handled by the fault-tolerant software design, and an incorrect airplane configuration may be detected by the verification process (described above). However, software manipulation can still threaten business of airplane owner.

Business threats. Late or false alarm detection of software manipulation, and denial of service attack on software distribution can all create unwarranted delays to flights and increase owner costs. Airplane owner business can also be impeded if attackers manipulate some software, such as cabin light system software (DO-178B Level D parts), to generate visible onboard system malfunctions and lower passenger confidence/convenience. Further, an eavesdropper can induce intellectual property costs by illegally distributing copyright-protected software.

C. Security Requirements

In order to address the two classes of threats, the following security primitives must be employed in AADS.

- *Integrity*: Software received by the airplane must be correct, i.e. as produced at its supplier. This ensures that manipulation of the content of distributed software is detected.
- *Authenticity*: Each software part by the airplane must be traceable to its source, i.e. any intermediate entity in the model and/or its supplier, and its freshness as well as intended destination must be verifiable. This ensures that a received part is not invalid, an outdated version, or a replayed/diverted part from another airplane's configuration.
- *Authorization*: The identity and corresponding privilege (e.g. allowed to send software part) of the source of software must be verifiable. This ensures that the received software is not invalid and enables traceability.
- *Non-repudiation*: Any action related to software distribution must be traceable to a verifiable originating entity.
- *Availability*: Should the network be unavailable, there must be backup mechanisms to distribute software to the airplane (e.g. physical transfer of CD/DVDs).

We refer the reader to Refs. 3 and 5 for a detailed exposition of the threats, requirements, and their adequacy in meeting specific threats in AADS.

D. Security Mechanisms

Digital signature with a timestamp offers a public key cryptography based mechanism for protecting integrity and authenticity of software parts, as well as satisfying non-repudiation. Further, we note that public key encryption can serve to protect confidentiality of software parts with intellectual property content when needed.

We note that virtual private networks (VPNs) do not suffice as a solution for AADS. A VPN authenticates the source and protects message integrity and confidentiality. However, message authentication is not provided. Therefore, a VPN cannot guarantee that software parts received are authentic. If an attacker sends a manipulated part over VPN, the destination will incorrectly accept it as a valid part as long as its integrity is verifiable.

In order to verify a signature, the corresponding public key must be retrieved from a digital certificate. The destination system receives the certificate along with the signed software part, enabling verification. A trusted party, called Certificate Authority (CA), assigns and distributes certificates, and forms an integral part of the public-key

infrastructure (PKI) supporting signatures.[8] Although this paper does not consider details of PKI, in Sections IV and V we discuss some of the challenges raised by PKI and public key based solutions. But first, we provide a concise overview of the ongoing practical developments in our work.

III. AADS Protection Profile, Implementation, and Security Evaluation

In Ref. 5, we have developed a formalized version of the proposed security framework for the AADS as a Common Criteria (CC) Protection Profile.[7] Based on an analysis of the information value of safety-critical assets (e.g. Level A software) and the nature of expected threats against the security of those assets, we have justified the minimum CC Evaluation Assurance Level (EAL) (see Ref. 7) for the AADS as EAL6. However, we have also determined that less critical software parts need only be assured at EAL4. Our analysis is validated by the Information Assurance Technical Framework (IATF), Chapter 4, "Technical Security Measures."[6]

Further, as noted in Ref. 2, Boeing is implementing a version of secure AADS, called Boeing Electronic Distribution of Software (BEDS) system, for secure electronic distribution of loadable software and data between 787-8 airplane model and ground systems. We are in the process of applying our framework to BEDS for analyzing and exhibiting the system's security properties. The established CC Protection Profile can enable us to develop a CC Security Target for evaluation of BEDS at the desired EALs.

IV. Challenges Presented by a Secure AADS

The proposed use of security solutions, such as digital signatures and certificates, is not new to Internet applications. E-commerce and financial institutions are aware of the returns from investing heavily in such security solutions for their online data transactions.[9] However, the use of security solutions in airplane applications is relatively new to the aviation industry. Several unprecedented challenges arise that must be addressed. For example, implementing security in applications while meeting the unique restrictions presented by onboard/off-board environments (e.g. the constraints of AADS in Section II.A). Another example is evaluation of the impact of secure applications on airplane manufacturers and owners (e.g. balancing added operational costs with expected returns from the security investment). We highlight the important challenges arising in the secure AADS.

A. Verifying Signatures at Traversed Airport w/o Network Connectivity

An airplane may traverse multiple airports during its end-to-end flight, requiring the ability to handle intermittent connectivity along its trajectory (constraint C1 in Section II.A). Further, at each airport traversed the airplane systems securely connect to multiple off-board systems, e.g. wireless networks and airline IT systems. Consequently, any candidate security solution for an airplane application must be scalable in terms of total number of communicating off-board systems. With use of digital signatures the problem reduces to ensuring airplane systems are able to verify certificates from these off-board systems. As shown in the top right side of Fig. 2, one solution approach is to use a proper PKI for online verification of certificates received by airplane systems. However, this approach is limited by the availability of networks at traversed airports. An alternative approach is to preload certificates in the airplane, providing offline verification of certificates. However, the scalability of this approach is limited not only by the number of communicating off-board systems, but also by the number of software suppliers as seen next.

B. Verifying Signatures from Multiple Suppliers and Owners

The AADS has multiple suppliers that produce software for an airplane and multiple owners may be present at any given airport (constraint C2 in Section II.A). In order to protect the software parts distributed from the suppliers, one solution approach is to make the airplane verify signatures of suppliers on the parts. Additionally, to ensure that the airplane accepts parts only from its authorized owner, the airplane must verify the owner's signature on the parts. As shown in Fig. 2, a supplier signs software parts, the owner verifies this signature and adds its own signature, and finally the airplane verifies owner's as well as supplier's signatures. However, such an approach may not be scalable if the airplane uses offline verification with preloaded certificates, since the certificate management complexity increases with the number of suppliers. Fig. 2 also illustrates that an alternative scalable approach is to make the owner verify and distribute the re-signed software parts, and make the airplane verify only the owner's signature using a preloaded certificate. Unfortunately, this approach may increase the overhead costs at the owner as discussed below.

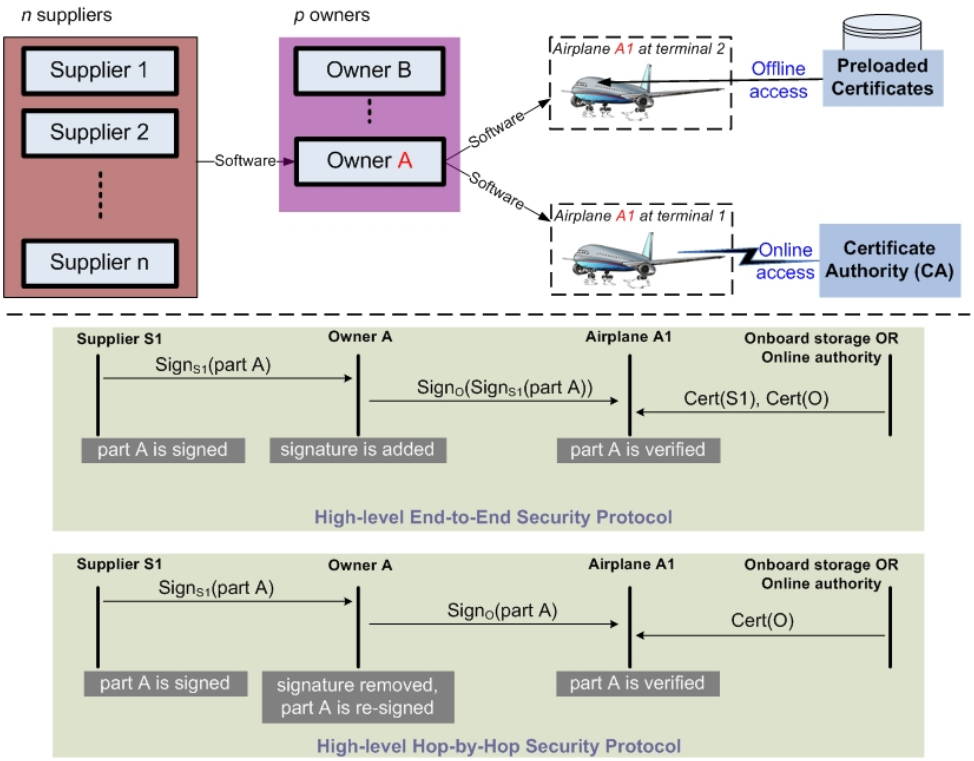

Figure 2. Illustration of proposed approaches meeting AADS constraints. The top half is a schematic of secure software distribution from suppliers to airplane using either preloaded certificates or proper PKI (CA) at airplane. The bottom half shows high-level protocols for secure software distribution with verification (end-to-end) or without verification (hop-by-hop) of supplier signature at airplane. $Sign_X(p)$ denotes signature of entity *X* on part *p*. Cert(X) denotes certificate of entity *X*.

C. Reducing Impact of Secure AADS at Owner

The RTCA DO-178B guidance indicates that the safety-criticality of airplane loadable software decreases from Level A to E.[1] However, AADS need not differentiate software based on these levels, rendering the same level of assurance for all. With an assurance level of CC EAL6 needed for systems handling safety-critical parts, it becomes necessary to evaluate the entire AADS at that assurance level. Consequently, the evaluation effort, which involves use of formal methods in security analysis, incurs significant costs and time.[7] For the approach described above where owner removes supplier signature and re-signs software, the evaluation effort of EAL6 is levied on both owner and supplier.

In order to reduce the impact at the owner (constraint C3 in Section II.A) a tradeoff can be achieved by making the owner retain supplier signatures on the safety-critical parts, and make airplanes verify these signatures. This approach reduces the security evaluation effort to a manageable portion, i.e. system signing parts at suppliers and system verifying parts at airplane. The burden of rigorously evaluating (at EAL6) the IT systems handling safety-critical parts at the airplane owner is eliminated. Another advantage of the approach is that it provides end-to-end integrity and authenticity protection for safety-critical parts. However, scalability issues with use of preloaded certificates discussed above must be addressed by the owner. Moreover, this approach also requires compliance and support from all the airplane loadable software suppliers.

Table 1 summarizes the proposed approaches and the accommodated AADS constraints. It can be observed that each approach has its tradeoffs. Overall, a hybrid solution to secure AADS while meeting its constraints can be constructed as follows: make supplier sign all software parts; make owner verify supplier signature and re-sign; make the airplane verify both supplier and owner signatures on the safety-critical software parts, and only owner signature on all other parts; and use proper PKI as well as preloaded certificates for verification of parts at the airplane. Determining the set of preload certificates is left as a challenging open problem.

Property / Scheme *(Signature + Verification on airplane)*	Intermittent Connectivity	Multiple Off-board Systems	Multiple Suppliers	Reduced Impact at Owner
Supplier + PKI	×	√	√	√
Supplier + Preload cert	√	×	×	√
Owner + PKI	×	√	√	×
Owner + Preload cert	√	×	√*	×

Table 1: Comparison of proposed schemes and satisfied AADS properties. √ - can accommodate. × - not guaranteed to accommodate. Scheme specifies the signature verified and verification mechanism at airplane. * - because owner verifies supplier signatures using a proper PKI on ground.

D. Specifying Impact of Security on Airplane Safety Regulations and Guidance

Consistent with the constraint C4 in Section II.A, the FAA recently acknowledged that when onboard networks connect to offboard systems, the airplane becomes a node on the Internet, and the existing airworthiness regulations do not include safety standards to address the emerging securing requirements.[10] Further, they explicitly state the need to secure the electronic distribution of loadable software.[11] On the other hand, regulatory agencies also understand that the introduction of digital certificates and cryptographic keys in onboard system storage clearly affects the airplane operator guidance. We discuss one specific impact next.

V. Open Problems and Future Work

A. Airline PKI Requirements

The public key based applications of eEnabled airplanes may levy new requirements on airplane operators. Consequently, airlines that currently do not fully support any PKI may need guidelines to cover the PKI requirements in airplane operations, such as management of certificates and cryptographic keys. In our future work, we will explore airline PKI needs and study applicability of solution approaches, including preloaded certificates not employing any trust chain between them, and employment of a proper PKI. We also intend to investigate evaluation cost-effective and high-assurance PKI models to support AADS.

B. Security of Airplane Health Management for eEnabled Airplanes

An unexplored area in eEnabled airplane is the security of onboard generated airplane data that is distributed to ground systems. We focus on the airplane health management (AHM) application.[2] In particular, we will explore the potential use of wireless sensor networks (WSNs) to sense, collect, and transfer health data, some of which will be distributed to off-board systems for further data analysis. AHM WSN can offer significant advantages to the airplane operator, including enhancing safety by real-time health monitoring of flight-critical systems, and reducing maintenance costs and delays by early detection of onboard system failures.[12] Another notable benefit is the reduction in system weight and costs associated with onboard wiring. In our future work, we will propose a security framework to enable the beneficial use of AHM WSN. We note that integration of this framework with the one proposed for AADS, offers end-to-end security for AHM data.

C. Security of Air Traffic Management for eEnabled Airplanes

Integration with air traffic management (ATM) centers is another potential application of eEnabled airplanes. Advances in wireless technologies, such as WiMAX,[13] enable broadband point-to-point connectivity over long distances between airplane and ATM center. By communicating with air traffic centers, an eEnabled airplane may not only improve air traffic control efficiency and reduce flight delays, but also automate processes prone to human errors (e.g. landing in low visibility conditions). Based on the security framework proposed in this paper, we will study security of ATM for eEnabled airplanes. However, unique security challenges arise due to application constraints such as online connection between the airplanes in-flight and the traffic centers.

VI. Conclusion

This paper focused on securing the electronic storage and distribution of airplane loadable software. We identified two classes of threats, one to airplane safety and another to business of airplane owners. After specifying

security requirements, we proposed use of digital signatures for end-to-end integrity and authenticity of the software distributed from supplier to airplane, presented the various challenges that must be addressed, and suggested a suitable architecture. The results of our work have profound implications for security of other emerging and potential eEnabled airplane applications, ranging from integration with ground-based maintenance information systems to interoperability with air traffic control. Identifying the criteria the regulatory agencies such as FAA must adopt or recommend with respect to the security of eEnabled airplane applications, remains an open problem that needs to be addressed.

References

[1] Radio Technical Commission for Aeronautics (RTCA), DO-178B: Software Considerations in Airborne Systems and Equipment Certification, December 1, 1992.

[2] G. Bird, M. Christensen, D. Lutz, and P. Scandura, "Use of integrated vehicle health management in the field of commercial aviation," *NASA ISHEM Forum*, 2005.

[3] S. Lintelman, R. Robinson, M. Li, D. von Oheimb, K. Sampigethaya, and R. Poovendran, "Security Assurance for IT Infrastructure Supporting Airplane Production, Maintenance, and Operation," *National Workshop on Aviation Software Systems* [online database], URL: http://chess.eecs.berkeley.edu/hcssas/papers/Lintelman-HCSS-Boeing-Position_092906_2.pdf [cited 19 April 2007].

[4] Eric Fleischman, Randall E. Smith, and Nick Multari, "Networked Local Area Networks (LANs) in Aircraft: Safety, Security and Certification Issues, and Initial Acceptance Criteria (Phases 1 and 2)," Final Report, December 2006.

[5] R. Robinson, D. von Oheimb, M. Li, K. Sampigethaya, R. Poovendran, "Security Specification for Distribution and Storage of Airplane-Loadable Software and Airplane-Generated Data," Common Criteria Protection Profile manuscript, available upon request.

[6] US National Security Agency, Information Assurance Technical Framework, Release 3.1, URL: http://www.iatf.net/framework_docs/version-3_1/ [cited 19 April 2007].

[7] Common Criteria portal. http://www.commoncriteriaportal.org/ [cited 19 April 2007]

[8] C. Adams and S. Lloyd, *Understanding PKI: Concepts, Standards, and Deployment Considerations*, 2nd edition, Addison-Wesley, 2003.

[9] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce*, Vol. 9, No. 1, 2004, pp. 69-105.

[10] Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing Model 787–8 Airplane; Systems and Data Networks Security—Isolation or Protection from Unauthorized Passenger Domain Systems Access, [Docket No. NM364 Special Conditions No. 25–07–01–SC], Federal Register, Vol. 72, No. 71, April 13, 2007 [online database], http://edocket.access.gpo.gov/2007/pdf/E7-7065.pdf [cited 19 April 2007].

[11] Federal Aviation Administration, 14 CFR Part 25, Special Conditions: Boeing Model 787–8 Airplane; Systems and Data Networks Security—Protection of Airplane Systems and Data Networks From Unauthorized External Access, [Docket No. NM365 Special Conditions No. 25–07–02–SC], Federal Register, Vol. 72, No. 72, April 16, 2007 [online database], http://edocket.access.gpo.gov/2007/pdf/07-1838.pdf [cited 19 April 2007].

[12] H. Bai, M. Atiquzzaman, and D. Lilja, "Wireless Sensor Network for Aircraft Health Monitoring," *Broadband Networks (BROADNETS'04)*, 2004, pp. 748 – 750.

[13] M. Barbeau, "WiMax/802.16 threat analysis," *ACM international workshop on Quality of service & security in wireless and mobile networks*, Montreal, Quebec, Canada, 2005, pp. 8--15.