SECURE NETWORK-ENABLED COMMERCIAL AIRPLANE OPERATIONS: IT SUPPORT INFRASTRUCTURE CHALLENGES

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, 81730 München, Germany

ABSTRACT

The next-generation commercial airplane models have networking facilities that enable onboard systems to communicate between themselves as well as with off-board systems. This new feature allows network applications to realize many benefits for airplane manufacturing, operations and maintenance processes. However, at the same time vulnerabilities are introduced that can threaten the onboard systems. Regulatory bodies such as the EASA and FAA recognize that the unprecedented network-enabled airplane model may impact long-established safety regulations and guidance. In this paper, we focus on securing a specific network application, i.e. the electronic distribution of airplane loadable software. The use of data networks provides opportunities for corruption of safety-critical and business-critical airplane software. The paper presents a security framework that we have proposed for identifying threats to the airplane software distribution, and mitigating them. Additionally, challenges to securing the distribution, and open problems in the security of network-enabled airplanes are discussed.

1. 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 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, for example in RTCA DO-178B[1], for assuring the quality of airplane loadable software during its design and development. The integrity of safety-critical software parts must not be compromised. However, the use of public networks for storing and distributing airplane software may expose vulnerabilities that can be exploited to attack 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 or 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.

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

The rest of the paper is organized as follows. Section 2 presents an overview of the proposed security framework. We present the AADS model, security threats to AADS, and requirements for mitigating the threats. We also outline a solution approach based on digital signatures that can provide end-to-end security for AADS. Section 3 discusses various unprecedented challenges presented by the secure AADS to airplane operators. Section 4 discusses open problems and future directions in the area of eEnabled airplane security, and Section 5 concludes.

2. A SECURITY FRAMEWORK FOR AIRPLANE SOFTWARE DISTRIBUTION

2.1. AADS Model

Fig. 1 shows the constituent entities in the AADS model. As illustrated, a supplier creates loadable software appropriately assured for safety, and distributes the software to an intermediate entity, i.e. the airplane manufacturer, owner (an airline) or third-party servicer. The intermediate entity stores the loadable software and distributes it to the airplane or to a next intermediate entity. An attacker may attempt to corrupt software by exploiting network and system vulnerabilities or as an insider at an intermediate entity. Additionally, we consider the following constraints (C1 through C4) on the AADS system.

- (*C1*) Fig. 1 illustrates that an airplane can traverse multiple airports with different networking capabilities. Each airport at which the airplane receives software may employ one among many available wireless standards for its network, or may not have any network connectivity whatever. 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 not be excessively costly.
- (*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.

As will be seen in Section 3, these constraints complicate the design of the secure AADS by requiring tradeoffs.

We assume that the airplane operator verifies the loadable software configuration to be correct after upload to onboard systems. Verification may be enabled by an airplane configuration list of software parts available to the operator. We also assume 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. Moreover, we assume that redundancy checks help prevent installing manipulated software on airplane LRUs. Nevertheless, threats to the service provided by AADS emerge as discussed next.

2.2. Security Threats

Data networks have vulnerabilities that can be exploited by attackers attempting to tamper with AADS operation.

Airplane safety threats. To lower safety margins of an airplane, attackers can attempt to manipulate and corrupt the airplane's safety-critical software parts (e.g. DO-178B Level A parts) during distribution. Safety threats are reduced to an extent by the error-detecting and fault-tolerant design of on-board systems. So the main safety threat is that coherent intentional manipulation of genuine parts or injection of fake parts by well-informed attackers could go undetected.

Business threats. Late detection of part manipulation, tampering with the AADS administrative messages (i.e., upload commands, inventory requests and related responses) which may lead, for instance, to false alarms, and general denial of service attacks on software distribution can all create unwarranted delays to flights and increase owner costs. An airplane owner's business can also be impeded if attackers manipulate non-safety critical

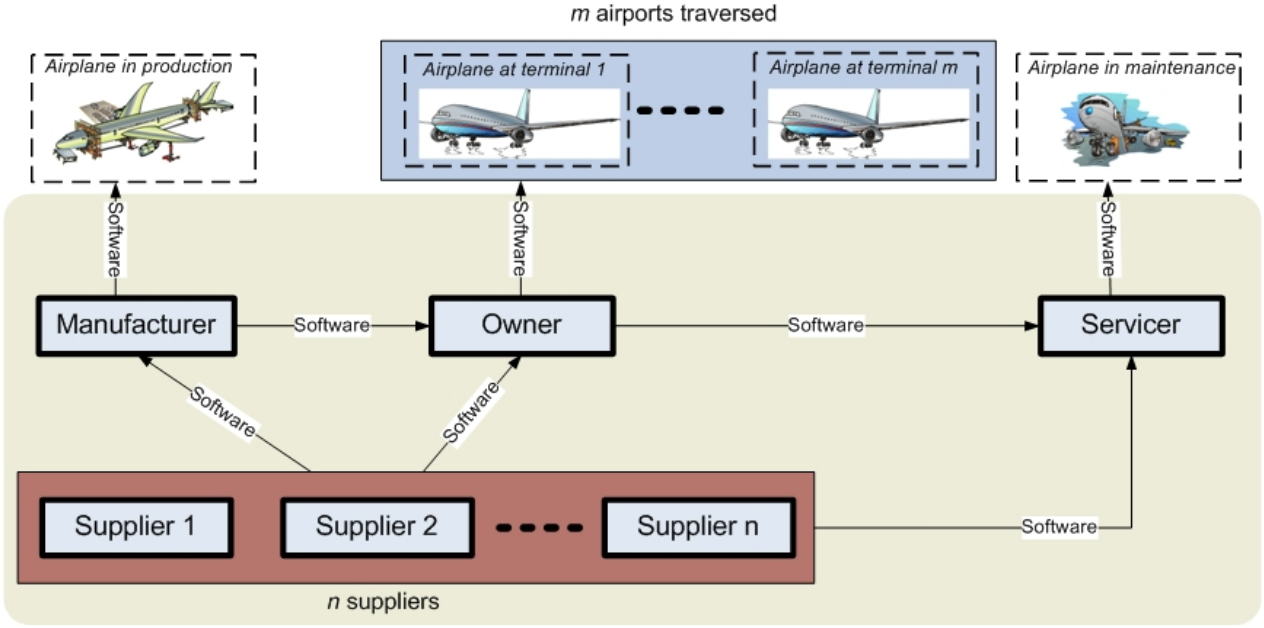

Fig. 1 - Illustration of the Airplane Asset Distribution System (AADS) model and its constraints, i.e. multiple suppliers delivering software to airplane, and multiple airports are traversed by airplane.

software, such as cabin light system software and other DO-178B Level D or E parts, to generate visible onboard system malfunctions and lower passenger confidence or convenience. Further, an eavesdropper can induce intellectual property costs by illegally distributing copyright-protected software.

2.3. Security Requirements

In order to address the two classes of threats, the following security requirements must be met by the AADS.

- *Integrity*: Software received by the airplane must be correct, i.e. as produced at its supplier. This ensures that any manipulation of the content of distributed software is detected. The part identity must be protected with the part, such that it can be enforced that (the right version of) the part is accepted at the right destination as desired by the airplane configuration management.
- *Authenticity*: Each software part by the airplane must be traceable to a trusted source, i.e. any intermediate entity in the model and/or its supplier.
- *Authorization*: The identity and corresponding privilege (e.g. allowed to send software part) of subjects attempting to perform critical actions must be verified. This helps ensure that the received software is valid and enables traceability.
- *Traceability*: Any action related to software distribution must be logged and attributed to a responsible entity.
- *Early Detection:* The fact that a part has been tampered with must be detected as early as possible (that is, by the next trusted entity handling it) to reduce propagation of invalid parts and minimize delays to obtain replacements
- *Correct Status Reporting*: Status information concerning asset use, in particular reports on the current contents of the airplane on-board parts storage and signature expiration information must be correct. This avoids, for instance, false claims about missing parts.
- *Availability*: As long as there is sufficient connectivity, AADS must ensure in-time delivery. 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 [3] and [5] for a detailed exposition of the threats, requirements, and their adequacy in meeting specific threats in AADS.

2.4. 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 traceability and even 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 (VPN) 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. For verifying the validity of the received certificate, the receiver can either use off-line verification with a trusted set of preloaded certificates or verification with a trusted third party called Certification Authority (CA). The preloaded certificates or CA public key, respectively, must be transported to the airplane using integrity protected out-of-band processes. The CA forms an integral part of a public-key infrastructure (PKI), with functions that include certifying the signing keys, and distributing certificates for these keys as well as checking their validity (revocation status)[8]. Although this paper does not consider details of PKI, in Sections 4 and 5 we discuss some of the challenges raised by PKI and public key based solutions.

2.5. Security Evaluation Requirements

We have developed a formalized version of our proposed security framework for the AADS[5] as a Common Criteria (CC)[7] Protection Profile. 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 Evaluation Assurance Level (EAL)[7] for the integrity and authenticity protection by the AADS as EAL 6. However, we have also determined that handling less critical software parts and the business-related security aspects require only EAL 4. Our analysis is validated by the Information Assurance Technical Framework (IATF)[6], Chapter 4, “Technical Security Measures”.

3. CHALLENGES TO SECURING THE AADS

The proposed use of security solutions such as digital signatures and certificates is not new to Internet applications. Financial institutions and other businesses engaging in e-commerce are aware of the returns from investing heavily in security solutions for their online data transactions[9]. However, the use of information 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 listed in Section 2.1). 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.

3.1. Verifying Signatures at Traversed Airport without Network Connectivity

An airplane may traverse multiple airports during its end-to-end flight, requiring the ability to handle intermittent network connectivity along its trajectory (constraint C1 in Section 2.1). Further, at each airport, airplane systems may be required to connect securely to multiple off-board

systems, e.g. wireless networks and airline IT systems. Consequently, any candidate security solution for airplane applications must be scalable in terms of total number of communicating off-board systems. With the use of digital signatures the problem reduces to ensuring airplane systems are able to verify certificates from these off-board systems. Therefore, even if backup mechanisms are used to transfer software to the airplane, the certificates received with the software still need to be verified. In this paper, we consider two extreme approaches for verification of the validity of certificates received by airplane systems, as shown in the top right side of Fig. 2, as well as their combination.

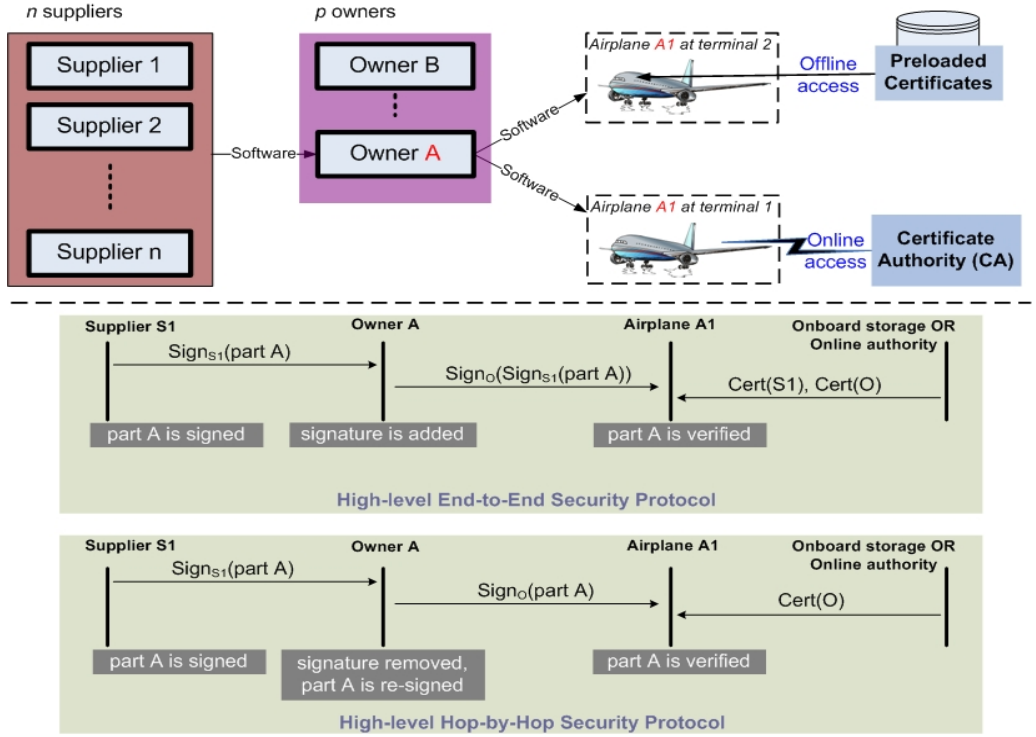

Fig. 2 - Illustration of proposed approaches meeting the AADS constraints. The top half is a schematic of secure software distribution from suppliers to airplane using either preloaded certificates or proper PKI (CA) at airplane. The bottom half shows high-level protocols for secure software distribution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

One approach is based on a PKI that provides online verification to check certificate validity or the latest certificate revocation lists to the airplane over the network. Obviously, this approach is limited by the availability of networks at traversed airports. On the other end of the spectrum is an approach that pre-loads certificates in the airplane, providing offline verification of signatures. However, with this approach, revocation of certificates is very limited and the scalability is limited by the number of communicating off-board systems and by the number of software suppliers, as seen next.

3.2. Verifying Signatures from Multiple Suppliers and Owners

The AADS comprises multiple suppliers that produce software for a given airplane. Multiple owners may be present at any given airport (constraint C2 in Section 2.1). In order to protect software parts distributed from suppliers, one solution approach is to have 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, each supplier signs its software parts, the owner verifies the owner 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 certificate management complexity increases with the number of suppliers. Fig. 2 also illustrates that an alternative, scalable approach is to have the owner verify and distribute re-signed software parts, while the airplane verifies only the owner's signature against a preloaded certificate. Unfortunately, this approach may increase the overhead costs at the owner, as discussed below.

3.3. Reducing Impact of Secure AADS at Owner

The RTCA DO-178B guidance indicates that the safety-criticality of airplane loadable software may range from Level A, safety-critical, to Level E, no safety impact[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

the owner removes supplier signatures and re-signs software, the evaluation effort of EAL6 is levied on both owner and supplier.

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. √* - accommodated if owner verifies supplier signatures using a proper PKI on ground.

In order to reduce the impact at the owner (constraint C3 in Section 2.1) a tradeoff can be achieved by having owners retain supplier signatures on the safety-critical parts, and making airplanes verify these signatures. This approach reduces the security evaluation effort to a manageable portion, i.e. the system signing parts at suppliers and the system verifying parts on the 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 AADS constraints accommodated by each. 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: have each supplier sign all software parts; ensure owners verify supplier signatures and additionally sign the parts; have the airplane verify the owner signature, and for safety-critical parts additionally verify the supplier signature.

For verification of the supplier signed safety-critical parts at the airplane, use a PKI that provides online verification of certificate validity, or at least provides the most recent certificate revocation lists to the airplane. In the absence of network connection, verify only the owner signatures, using pre-loaded certificates.

Determining the set of preloaded certificates for verifying certificates from off-board systems connecting with the airplane remains as a challenging open problem.

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

Consistent with the constraint C4 in Section 2.1, the FAA recently acknowledged that when onboard networks connect to off-board systems, the airplane effectively becomes a node on the Internet. Existing airworthiness regulations do not include safety standards to address the resulting security requirements[10]. Further, they have explicitly acknowledged 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 airplane operator guidance. We discuss one specific impact next.

4. OPEN PROBLEMS AND FUTURE WORK

4.1. Implementing and Evaluating the AADS

As noted in [2], Boeing is implementing an instance of AADS, called Boeing Electronic Distribution of Software (BEDS) system, for secure electronic distribution of loadable software and data between airplanes 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[5] will enable us to evaluate BEDS against a specific CC Security Target derived from the generic Protection Profile.

4.2. Airline PKI Requirements

The public key based applications of eEnabled airplanes levy new requirements on airplane operators. Consequently, FAA and the European Aviation Safety Agency (EASA) have mandated that operator guidance be suitably modified to include PKI requirements, such as management of certificates and cryptographic keys. In our on-going work, we are exploring airline PKI needs and studying the 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.

4.3. Security of Airplane Health Management for eEnabled Airplanes

An unexplored area in eEnabled airplane is the security of airplane-generated 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 analysis. An AHM WSN can offer significant advantages to airplane operators, 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.

4.4. 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 the security of ATM for eEnabled airplanes. However, unique security challenges arise due to application constraints such as online connection between in-flight airplanes and the traffic centers.

5. CONCLUSION

This paper focused on securing the electronic distribution of airplane loadable software. We identified two classes of threats, to airplane safety and to the business of airplane owners. After specifying security requirements, we proposed use of digital signatures for end-to-end integrity and authenticity of software distributed from a supplier to an airplane. We presented the main challenges to securing the electronic distribution of airplane software, and suggested a suitable architecture that addresses these challenges. The results of our work have profound implications for security of other potential eEnabled airplane applications, ranging from integration with ground-based maintenance information systems for flight logistics and maintenance, to interoperability with air traffic control. Identifying criteria that regulatory agencies must adopt or recommend with respect to the security of eEnabled airplane applications, remains an open problem.

6. ACKNOWLEDGEMENTS

We would like to thank Prof. Peter Hartmann from the Landshut University of Applied Sciences for his insightful and valuable comments that helped us to improve specific sections of this paper.

7. REFERENCES

[1] DO-178B: Software Considerations in Airborne Systems and Equipment Certification. Radio Technical Commission for Aeronautics (RTCA) (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* http://chess.eecs.berkeley.edu/hcssas/papers/Lintelman-HCSS-Boeing-Position_092906_2.pdf (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] Information Assurance Technical Framework, Release 3.1. US National Security Agency. http://www.iatf.net/framework_docs/version-3_1/.

[7] Common Criteria. http://www.commoncriteriaportal.org/

[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, http://edocket.access.gpo.gov/2007/pdf/E7-7065.pdf

[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, http://edocket.access.gpo.gov/2007/pdf/07-1838.pdf.

[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.