HIGH-ASSURANCE SDR-BASED AVIONICS RFID SYSTEM

Rainer Falk[*], Florian Kohlmayer[*], Andreas Köpf[*], Mingyan Li[†], Radha Poovendran[‡]
[*]Siemens AG Corporate Technology, Munich, Germany; [firstname.lastname]@siemens.com
[†]Contact Author: Boeing Phantom Works, Seattle, United States; mingyan.li@boeing.com
[‡]University of Washington, Network Security Lab, Seattle, United States; rp3@u.washington.edu

ABSTRACT

This novel architecture supports various future eEnabled airplane applications based on RFID technology. As RFID readers and wireless communication equipment is installed on-board of airplanes, it has to support a manifold of different wireless communication standards. The flexibility offered by Software Defined Radio (SDR) plays here an essential role. The security solution concept identifies the security building blocks needed to protect the SDR-based avionics RFID system.

1. INTRODUCTION

The emergence of fully network-capable or "eEnabled" commercial airplanes is a revolutionary step in Avionics Industry and has opened a great opportunity for a wide range of network applications, including airplane health management by connecting on-board sensor networks with data processing center on the ground, and airline logistics facilitated by the communication between on-board RFID infrastructure and ground systems.

Along with the opportunity, an eEnabled airplane also imposes technical challenges on the realization of the network applications as it changes the assumptions made by conventional solutions. For example, today's RFID systems are typically designed for a specific application and deployed and managed by a single party. We envision that future on-board RFID systems of eEnabled airplanes will be dynamically connected to different ground systems for multiple purposes such as logistics, maintenance, and access control. Apart from tags and readers, the RFID infrastructure includes back-end servers spanning multiple administrative domains. One foreseeable benefit of this multi-purpose RFID system is that it supports airplane weight reduction as one single RFID System can support various applications.

The main contribution of this paper is a collaborative investigation between Boeing Phantom Works and Siemens Corporate Technology into such a mobile, wirelessly connected multi-purpose on-board RFID system, where the reader infrastructure is integrated with ground-based systems. In order to flexibly support different wireless ground communication systems and adapt to various RFID standards, we propose to use Software Defined Radio (SDR) as the underlying technology in the multi-purpose RFID system. Software Defined Radio (SDR) is a reprogrammable or reconfigurable radio technology with benefits such as support of forward compatibility for accommodating upcoming communication technologies. As just one hardware module is needed for multiple wireless standards also a weight advantage is realizable.

We present a novel architecture for an RFID system in which the flexibility offered by SDR plays an essential role to support various future eEnabled airplane applications. The key to the successful adoption of such an RFID system depends on the ability to provide authenticity and end-to-end integrity of the information collected from RFID tags, transported by readers, processed and stored by middleware and/or backend servers. Furthermore, SDR technology can pose security threats to the radio network through intentional or unintentional reconfiguration of its radio frequency parameters and link-layer stack. We perform security analysis on the SDR-based RFID system, identify potential vulnerabilities, and present security building blocks.

After outlining two application scenarios in Section 2, we describe the SDR-based avionics RFID system in Section 3. In Section 4, we present the main security solution components, including the protection of distributed RFID processing, the protection of wired and wireless communication extending between different stakeholders, and the secure reconfiguration of SDR equipments, i.e. the onboard RFID readers and the onboard wireless access component. We conclude with an overview on related work in Section 5 and an outlook to future work in Section 6.

2. APPLICATION SCENARIOS

Exemplary RFID application scenarios are described here to illustrate and motivate the technological work. It should, however, be noted that the intention is to provide a generic RFID infrastructure that can be used flexibly for various applications. Actually, as the specific RFID applications

used at various airports cannot be known in advance, the objective is to design a RFID system in such a way that it is not limited to certain, known, existing applications.

2.1 Airport Logistics Asset Tracking

One of the motivating applications is asset tracking at airports. The location of objects and persons shall be tracked to improve logistic processes. Examples of assets are containers, baggage, vehicles, tools, personnel (crew, service personal, maintenance) on both the airfield and on-board of an aircraft, and also spare parts and maintenance tools. Interesting applications areas are in particular logistical processes as cleaning, catering, and maintenance. RFID tags can also be used to authenticate an airport's maintenance and service personal, and possibly even used tools when getting on-board of the aircraft. Another application scenario is to ensure that all tools are off the airplane when maintenance is complete.

2.2 Manufacturing

At a certain point during the manufacturing process, the future aircraft will include RFID reader devices that may be integrated with a fixed RFID infrastructure. However, a different view is to use special mobile, wirelessly connected RFID readers for the manufacturing process; In contrast to existing RFID systems, not only RFID tags are attached to movable objects, but some of them such as the aircraft body, a wing, or crawlers would contain also mobile, wirelessly connected RFID readers. The mobile readers provide the advantage of extending the possibility of inventory tracking and supervising logistic processes into areas, inside the aircraft, that could not be covered by a fixed RFID reader infrastructure located in the manufacturing hall.

During the manufacturing process many different scenarios are of interest. Examples are the matching of parts to their real world positions on the aircraft, access control and time management of employees, self organizing crawlers for efficient manufacturing, automating process control, facilitating the generation of status reports, or simply locating personal and equipment.

3. SDR-BASED AVIONICS RFID SYSTEM

Taking the example of airport logistics, Fig. 1 shows the system and the involved entities.

The *On-board RFID Processing System (ORPS)* handles the RFID events within the airplane. It performs event filtering, basic pre-processing and aggregation to determine which

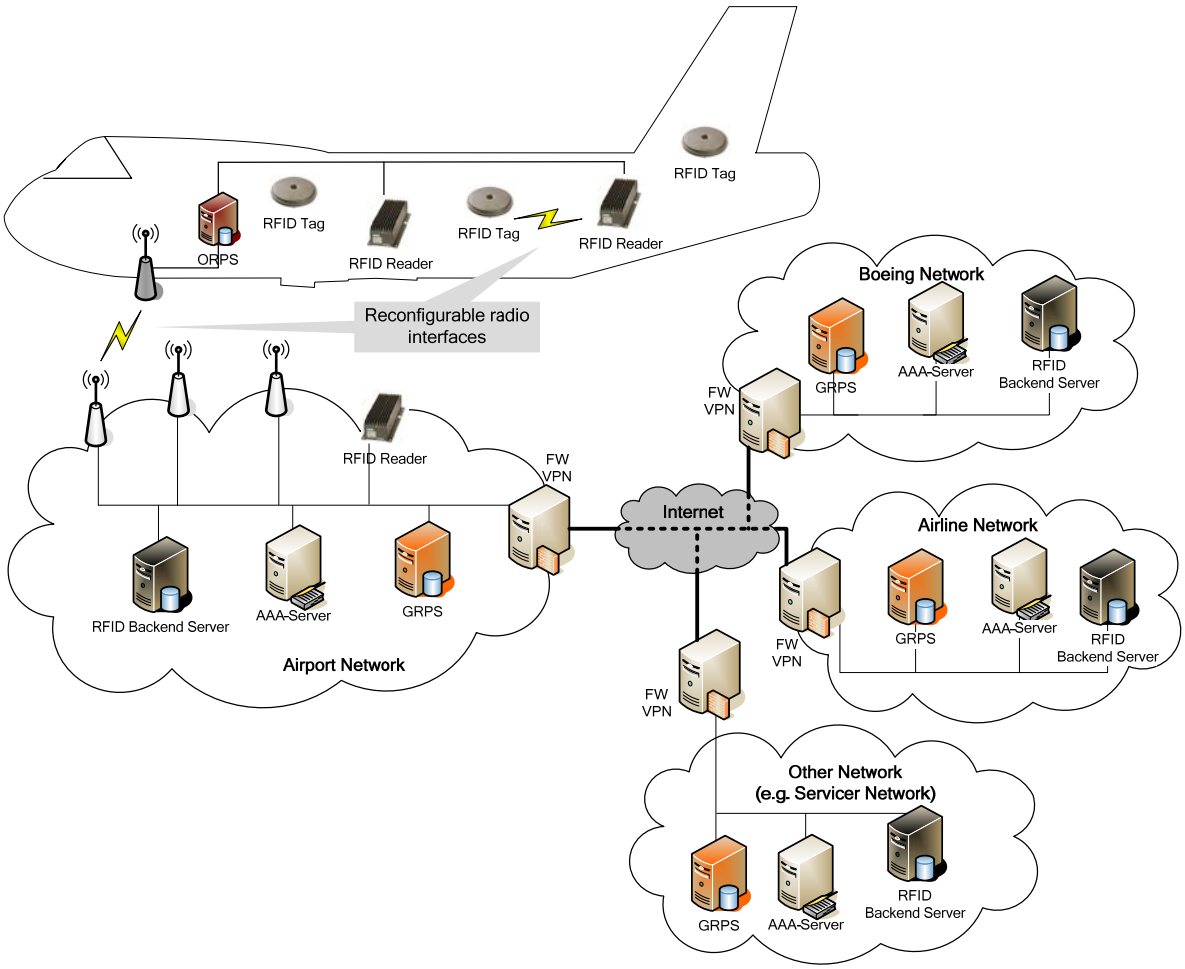

Figure 1: Mobile Multi-Purpose RFID System

RFID events have to be handled on-board and which events are delivered to the which ground system for processing. It also processes RFID events that are utilized by the aircraft itself. It manages the configuration of on-board RFID readers and the wireless connection to the ground-based backend RFID systems. It may provide additional functionalities, in particular firewall / traffic filtering, establishment of cryptographically protected tunnel, and mobility support (e.g. Mobile IP).

In order to support a set of wireless communication standards, we propose to use Software Defined Radio (SDR) for the communication between on-board and ground systems. SDR can also be leveraged to support heterogeneous RFID communication standards. Software reconfigurable radio provides a flexible path to support a large number of different wireless systems, both existing ones and future ones. Therefore it is also an approach to ensure compatibility with future standards. The future-proof is important as wireless aircraft communication equipment is used much longer than typical IT innovation cycles. Upcoming wireless communication standards can therefore be supported easily by installing a software update on existing equipment. The ORPS will be in charge of the reconfiguration job of both wireless interfaces, i.e. of the RFID interface and the wireless communication interface towards the ground systems. The actual software module will be provided from the ground system. Here exists the well known problem that first the required radio reconfiguration software has to be obtained before the corresponding radio standard can be activated [1]. In case of the known airplane route the radio software can be pre-loaded on the departure airport.

The *Ground RFID Processing System* (GRPS) is the counterpart to the airplane-based ORPS. It handles the events it receives from the ORPS as well as the local RFID events. Typically, fixed RFID readers will be installed at the airport and handled directly by the GRPS. Remote connections from the airplane to the fixed installed readers are enabled via the GRPS. At the airport network, AAA (authentication, authorization, and accounting) infrastructure is also available in order to establish a secure wireless link between the airplane and the airport network.

Remotely located RFID processing systems may be connected by secured VPNs. The VPNs can be established directly between involved network border devices ("firewall", depicted as FW/VPN devices in Figure 1). When needed, they can also be realized directly between the local and remote GRPS servers, or between the on-board ORPS and the respective GRPS server.

As the GRPS is the first point of contact for the airplane RFID processing system to connect with the ground infrastructure network, it can serve also as distribution point for the reconfiguration software. It can be connected with an airline's repository containing the software modules needed for various airports. It is envisaged that the airplane is equipped with SDR enabled radio modules that can be reconfigured to various wireless communication technologies used at different airports.

Different segments may be separated by firewalls. For example, in the airport network there may exist a firewall between the WLAN access points and the RFID backend system GRPS. Besides providing secure VPN tunnels, these firewalls may also perform network address translation (NAT) and filter network traffic. To support NAT/firewall traversal, resulting restrictions have to be considered, such as that – depending on the NAT/firewall configuration – only outgoing connections are allowed, that some protocols are entirely blocked, or that IP addresses and port numbers are altered.

4. SECURITY SOLUTION BLOCKS

A main objective of the work described in this contribution has been to identify required security requirements and propose solution blocks. This section describes the security issues for the RFID system outlined above and presents security building blocks to address them.

The intrinsic characteristics of the application environment impose specific and challenging security issues such as mobile RFID readers, multi-standard RFID tags, heterogeneous wireless communications, and dynamic security association. In fact, identifying new security issues in future RFID application systems is one of our research objectives. Many of the security challenges come from the fact that RFID readers are mobile on a global basis when mounted on-board of aircraft. They have to be reconfigured to support various different RFID ground systems that are connected wirelessly. In our proposed solutions, Software Defined Radio (SDR) plays a central role to provide the flexibility to reconfigure to different RFID and wireless access communication systems. Furthermore, the so far rather static security relationships between RFID reader and processing systems become dynamic, and the RFID processing itself involves different stakeholders spanning administrative domains.

In our proposed architecture, the security solution is comprised of security solution blocks that address different functionalities of the overall system. The main security requirements for which corresponding security building blocks are needed are:

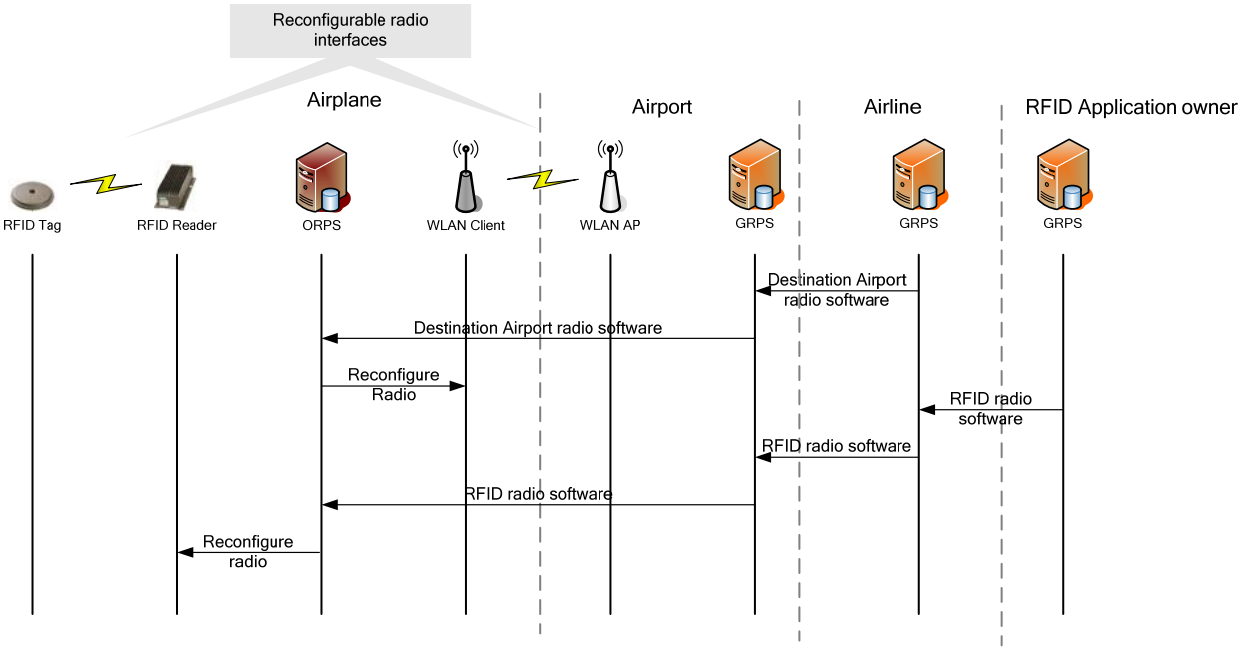

Figure 2: Exemplary Reconfiguration Chart

- SDR Security: In order to support multiple wireless standards, wireless communication equipments have to be reconfigured securely to be compliant with the locally used radio standards as well as with the local regulatory requirements.
- Secure RFID processing: To ensure correct RFID event processing, the distribution and processing of RFID readings are needed to be performed in an integrity-protected and authenticity-ensured way. RFID events may need to be processed in a distributed manner across multiple systems, including both on-board processing systems, and the dynamically discovered airport RFID processing servers. Secure RFID processing also ensures that RFID events are processed in the intended systems.
- Communication security: Wireless access authentication for establishing securely the wireless connectivity between the aircraft and the airport network. Communication between diverse RFID readers and processing systems that span multiple administrative domains has to be protected.

4.1 SDR Security

The main objective of SDR security is to ensure reliable and correct software reconfiguration for the radio to be compliance with respective regulatory rules and communication standards. That is, to ensure authorized installation and activation of correct software, authorized configuration management, and correct and authorized software updates.

4.1.1 SDR Configuration Authorization

Only authorized radio configurations and software modules may be executed. A digital signature of the software modules protects its integrity and assures that it originates from an authorized radio software provider. To comply with locally different regulations, it has to be respected that some radio configurations are permitted to be activated only in certain regions. This information is preferably included in the software module as meta information. Additionally the activation has to be context sensitive that the radio isn't for example activated during flight.

4.1.2 SDR Reconfiguration Control

The configuration of on-board SDR-enabled communication equipment (RFID, wireless access) has to be reconfigured to match the technologies at the current airport/manufacturing site. Authentication and access control ensure that only authorized entities, e.g. the airline, can modify the reader configuration profiles and download and install new radio software. As in the avionic scenario multiple stakeholders are involved the control is distributed. The current airport legal framework applies as well in which the airline is responsible for its airplanes. Additionally the airport may have an interest in controlling which wireless radio technology is supported by an airplane to ensure that it matches the respective airport's wireless standard. Also the use of various RFID applications requires different RFID radio standards which the RFID application stakeholder has an interest to configure. In the architecture described in Figure 1 the ORPS is in charge of the configuration management and as the ORPS needs to have all of the needed information (e.g. local GPS position, current airport regulations, requested RFID readings, available wireless connections to the airport). The ORPS is responsible for switching between the possible radio standards. In our design it is envisaged, that the ORPS can operate most of the time autonomous without waiting for the GRPS for reconfiguration triggers. This consideration is independent of the fact if the reconfiguration software is pushed to the ORPS or if the ORPS has to pull its needed software modules beforehand from the GPRS. To benefit from the

predictability of the routes and stops of an airplane, the reconfiguration software modules could be dedicated to specific airports and time frames only. As two different wireless interfaces are reconfigurable the actual reconfiguration process could be done in a two step approach, in the first step the connectivity to the infrastructure at the destination has to be assured and then in the second step the RFID interface could be reconfigured using locally available modules.

4.1.3 Airplane Assets Distribution System

Working groups in the airline industry define solutions for electronic distribution of digital assets (data software) [2]. Current and future network enabled airplanes support over-the-air software and data downloads and upgrades. The electronic distribution of airplane information assets is called Airplane Assets Distribution System (AADS) [3]. The AADS gets an asset from its producer, e.g. supplier or airplane and finally delivers it at its destination, i.e., embedded systems such as a Line Replaceable Unit (LRU) in an airplane, or at the consumer of airplane-generated data. The system is designed for distribution of generic assets and can therefore also be used for the download of SDR configurations and the delivery of software modules to the respective on-board systems.

4.1.4 Policy Management

The GRPS, in the various domains, and the ORPS entities are in charge of the reconfiguration process. Each GRPS in the authorization chain can modify, add, and delete the provided reconfiguration software, therefore only the ORPS in the end is responsible activating the appropriate and allowed radio. The policy can be also loaded dynamically by the airline. To execute policy rules, the needed information is embedded in the reconfiguration software itself and is known from the actual context the airplane is in.

A possible reconfiguration authorization chain is depicted in Figure 2. The airline is responsible for the proper functioning of the airplane software therefore all reconfiguration software has to traverse the airlines GRPS for making authorization decisions. The access software for the destination airport is sent via the current airport to the airplane, which can configure, after additional policy checks, the wireless access interface for the destination airport. The case is different for RFID radio reconfiguration. The RFID radio reconfiguration software is provided by the RFID application owner, i.e. the entity that deployed a certain RFID application system. It knows the used radio technology. Additionally, the airline being responsible for the aircraft has to authorize the usage of the RFID reconfiguration software. After performing these policy checks, the aircraft reconfigures the RFID readers accordingly.

4.2 RFID Security

4.2.1 Distributed RFID Event Processing

Information read from RFID tags is handled by different RFID processing systems. For example, it may be processed locally within the airplane, at the airport, and/or at a remote system belonging to the airline or the manufacturer. When a RFID tag is read by the airplane's reader system, the read information can be sent to the respective RFID processing system. Splitting of RFID events to the respective RFID processing system can be performed by any processing system: They can be split on-board of the aircraft, or all RFID events can be forwarded to a central airport server to which the different RFID application servers have access and can register for events of interest. A drawback of the centralized solution is that the airport obtains knowledge of all events occurred in the airport, independently of whether the airport is actually involved in the respective RFID application.

The splitting of RFID events has to be performed such that the events are delivered to responsible processing servers. Protection of communication to prevent manipulation and eavesdropping of RFID data is not sufficient, it has also to be ensured that at least critical RFID events are delivered only to the intended RFID processing system.

4.2.2 Split RFID Reader

A specific building block is the split RFID reader architecture. The on-board reader system may not have access to security credentials protecting RFID tag communication. Therefore, the RFID protocol between tags and readers may be executed using a split reader architecture: The on-board reader part realizes the radio interface, while the upper-layer RFID data is processed remotely.

4.2.3 RFID Tag and Middleware Security

Besides a secure connection via a protected communication channel between the related entities, security concerning the data stored on the RFID tags is an important issue as well. In its basic functionality an RFID tag is some kind of data storage – pretty much like a CD or floppy disk. The difference is that the amount of date stored on a tag is typically very limited when compared to a CD or floppy disk. But with increased functional range (i.e. attached sensors, location data, etc.) also the needed memory capacity increases. The increased available storage consequently results in higher attack potential. It is, for example, possible to put malicious code like a so called trojan horse, computer virus or network worm onto an RFID tag [4]. Subsequently such malicious code could easily get propagated to the backend infrastructure. This is not only an academic but a very practically relevant issue.

To mitigate this exposure, effective filtering and data evaluation are essential. This could be achieved by an adequate middleware solution. Middleware software manages the RFID readers and the data coming from the RFID tags, and passes the data to the backend systems. These tasks could be performed by the ORPS and/or the GRPS component.

4.3 Communication Security

4.3.1 Wireless Access Authentication

The connection between the airplane and the airport network has to be established securely. For the connection, various wireless standards such as WLAN, WiMAX and cellular technology are available. The main focus is 802.11 WLAN, albeit other technologies may be options for airports without WLAN infrastructure.

Secure WLAN network access can use, besides a pre-shared key suitable for home networks, an EAP-based network access (extensible authentication protocol) authentication. The client's supplicant is authenticated by a central authentication server (AAA server). The authenticator function of the WLAN access point receives the result whether the authentication was successful together with a secret session key (MSK, master session key) that is used to protect the wireless link between supplicant and authenticator

4.3.2 Protected Communication

Cryptographic tunnels protect the communication between different ground networks (e.g. airport, airline, Boeing), but as well as between the airplane system (ORPS) and the diverse ground networks (GRPS). As tunnels traverse network edges, possibly existing middle boxes like firewall and NAT (network address translation) devices have to be traversed. Relevant technologies for realizing such tunnels are virtual private networks (VPNs) based on IPsec or SSL/TLS. The security associations needed for IPsec can be established dynamically by the IKEv2 [5] protocol that supports beside pre-shared keys and certificates also EAP.

Protected communication is based on security agreements between involved entities. These are reflected by configuration data allowing the establishment of cryptographic security associations and defining allowed traffic flows. These agreements can be statically pre-configured, or they can be established dynamically based on pre-defined policy templates. The dynamic instantiation can be done on-demand, but more probably an automated establishment tool is used to set-up the various security associations efficiently with minimal administrative effort.

5. RELATED WORK

Applications and corresponding security issues of mobile RFID readers are presented in [6]. A mobile RFID reader is a PDA or mobile phone having an integrated RFID reader and wireless connectivity to infrastructure servers. Location-based services, enterprise applications, and private applications different security requirements are distinguished. A security architecture is described for location-based services in which the mobile network operator is relied upon to protect RFID transactions.

The objective of the Wireless Airport Association (WAA) is to expand wireless services at airports by providing recommendations, models, and best practices [7].

6. OUTLOOK

The paper described a visionary environment for future RFID applications that pose several challenges on required solutions. In this paper, scenarios and the basic architecture have been defined, and required technological security building blocks have been identified. Currently, specific security solutions building on and extending current state-of-the-art security technology are being investigated in more detail and mapped to components of the defined system.

7. REFERENCES

[1] End-to-End Reconfigurability (E2R) II, "Evolution of Reconfiguration Management and Control System Architecture," Deliverable D2.1, June 2006. http://e2r2.motlabs.com/Deliverables/E2RII_WP2_D2.1_060807.pdf

[2] ARINC, "ARINC Electronic Distribution of Software (EDS) Working Group." http://www.arinc.com/aeec/projects/eds/

[3] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, J.-U. Bußer, and J. Cuellar, "Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety," SAFECOMP, Springer, 2007. http://david.von-oheimb.de/cs/papers/SAFECOMP07.html

[4] M. R. Rieback, P. N. D. Simpson, B. Crisp, and A. S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?" in *IEEE PerCom 2006*, 2006. http://www.rfidvirus.org/papers/percom.06.pdf

[5] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," RFC 4306 (Proposed Standard), Dec. 2005. http://www.ietf.org/rfc/rfc4306.txt

[6] D. M. Konidala and K. Kim, "Mobile RFID Security Issues," Symposium on Cryptography and Information Security SCIS, Hiroshima, Japan, IEICE, January 2006. http://caislab.icu.ac.kr/Paper/paper_files/2006/Divyan_SCIS06.pdf

[7] WAA, "Wireless Airport Association (WAA)." http://www.wirelessairport.org/