Chapter 8.11
Certificate-Based Trust Establishment in eEnabled Airplane Applications: Challenges and Approaches

Mingyan Li
Boeing Research & Technology, USA

Krishna Sampigethaya
Boeing Research & Technology, USA

Radha Poovendran
University of Washington, USA

ABSTRACT

This chapter describes potential roles of trust in future aviation information systems. The next-generation air transportation systems are envisioned to be a highly networked environment with aircraft digitally linked with ground systems and wireless technologies allowing real-time continuous sensing, collection and distribution of aircraft information assets. The resulting enhancements promise to revolutionize manufacturing, operation and maintenance of commercial airplanes. Safe and dependable aircraft operation as well as public well-being in these complex system-of-systems with multiple stakeholders, demands that the distributed information assets can be trusted to be correct and that the level of trustworthiness in systems can be established. This chapter considers two recent abstractions of such aviation systems – an electronic distribution system connecting aircraft with ground components for exchanging updates and data of onboard software, and a radio frequency identification (RFID) system for logistics and maintenance of aircraft – which use digital certificates to establish trust in integrity and authenticity of information assets as well as in authorized components handling these assets. The chapter presents unique challenges of aviation, such as regulations and business models, which can complicate implementation of certificate-based trust and further warrant trustworthiness proofs.

DOI: 10.4018/978-1-61350-101-6.ch811

INTRODUCTION

The emergence of the fully network-capable, also referred to as "eEnabled" airplane is a significant leap in the commercial aviation industry, introducing a wide range of applications which use computer networks and wireless links to perform automated seamless exchange of information assets between aircraft and ground systems. Some major examples for aircraft information assets include field-loadable software updates from onboard equipment manufacturers, aircraft health status data from onboard sensors, logistics and maintenance history data from onboard systems and parts (Bird, Christensen, Lutz, & Scandura, 2005). Furthermore, emerging wireless technologies, such as Radio Frequency Identification (RFID), offer unprecedented improvements for aircraft operation and maintenance by providing ways to automate data sensing, storage, update and retrieval.

Together, the advances brought by eEnabled airplanes promise to enhance the safety, efficiency and reliability of the next-generation air transportation systems. Some recent real-world examples include the electronic delivery of aircraft software and data which replaces the cumbersome and often expensive management and physical transfer of floppy disks, CDs, and signed documents via bonded postal services (Spenser, 2005); maintenance of onboard hardware using low-cost passive RFID tags and readers which replaces the inefficient and error-prone barcode scanners (Porad, 2005).

Along with the beneficial opportunities, an eEnabled airplane imposes new challenges on the realization of the network applications as it changes the assumptions and shifts the paradigm our existing solutions are based on. For example, physical delivery of airplane software and data via FedEx assumes trustworthiness of the transport Sneakernet. Such an assumption is violated in electronic airplane software distribution, as computer networks such as Internet have well-known vulnerabilities which must be mitigated for secure airplane operation and airline business (FAA1, 2007; FAA2, 2007). In another example, today's RFID systems are typically designed for a specific application, deployed and managed by a single party. On the other hand, future onboard RFID systems of eEnabled airplanes are envisioned to dynamically connect with different ground systems and to serve multiple purposes such as logistics, maintenance, and physical access control. At the same time, safety-criticality of onboard aircraft information mandates protection of the integrity and authenticity of information flow in aviation RFID systems.

eEnabled airplane applications generally span multiple business domains. For instance, airplane software distribution involves multiple onboard equipment and airframe manufacturers who supply software and updates for aircraft, the airlines which maintain software configurations of its fleet, and the network-capable airplane which receives software and generates configuration reports. A fundamental challenge in building secure solutions for such cross-domain distributed network applications is to establish trust among different business parties that may not have pre-established business relationships and trust.

This chapter considers electronic airplane software distribution and airplane multi-purpose RFID systems as two examples, to illustrate challenges and approaches for security solutions and certificate-based trust establishment among entities for eEnabled airplane applications. The next section gives a concise background on eEnabled airplanes and their security, followed by two sections that present the challenges and approaches to securing airplane software distribution and RFID systems for eEnabled airplanes.