High Assurance Aerospace CPS & Implications for the Automotive Industry

Scott A. Lintelman[1], Krishna Sampigethaya[1], Mingyan Li[1], Radha Poovendran[2], Richard V. Robinson[1]
[1] Boeing Phantom Works, Bellevue, WA 98008
[2] Network Security Lab (NSL), University of Washington, Seattle, WA 98195

***Abstract*—The future "eEnabled" airplane, capable of participating as an intelligent node in a global information network, is a cyber-physical system (CPS) that requires real-time, continuous and concurrent monitoring as well as control. Vulnerabilities, however, can emerge from the integration of the eEnabled airplane with cyber-infrastructure such as the onboard embedded systems, the ground IT systems as well as other airborne systems. Consequently, high confidence is required for reliable, secure and efficient operation of this next-generation aerospace CPS. This paper presents challenges in addressing the problem of assuring distribution of avionics software and data between ground and the eEnabled airplane. Corruption of any of these information assets can threaten the operation of the CPS. We anticipate that technological innovations in high assurance CPS can mutually benefit aerospace and automotive industries.**

I. INTRODUCTION

Commercial aviation is at the threshold of a promising era brought about by the "eEnabled" airplane. The eEnabled airplane of the future can be envisioned as an aerospace cyber-physical system (CPS) possessing RFID tags, sensors and actuators that are embedded with onboard hardware and connected to avionics. Further, this CPS will have network access points to communicate with ground stations and airborne systems, enabling real-time, continuous monitoring of its health and control of its operation, as well as update of its onboard software and data. These unprecedented features of the CPS can revolutionize applications, such as aircraft health management, air traffic control, and distribution of loadable software and data [1], [2], [3].

In the automotive industry, recent trends in intelligent transportation systems can be evidently mapped to eEnabling in aerospace. Specifically, rapid advances in vehicular networks that enable the intelligent vehicle to participate in an information-rich roadway infrastructure for improving safety and efficiency of road travel [4]. We consider the network-enabled intelligent vehicle as an automotive CPS with applications that have counterparts for the aerospace CPS, e.g., collision avoidance and embedded system software delivery [4]. Therefore, innovations for emerging problems of the aerospace and automotive CPS may find mutual benefit.

In this paper, we address information assurance of aerospace and automotive CPS. Vulnerabilities in networks and technologies integrated with the CPS may disrupt the safe and beneficial functioning of the CPS by providing opportunities for attacks on information assets during their lifecycle [10]. For example, malicious corruption of software/data during distribution or health diagnostics during collection [3]. Therefore, identification, assessment and mitigation of threats to assets are pivotal for successful integration of the network-enabled CPS.

This paper summarizes our work on securing the distribution of aerospace CPS assets [3][5]. We are designing, developing, implementing and deploying a system that can securely deliver loadable software as well as data such as navigation database and configuration reports, to and from airplane. For evaluating this system, we have established a framework based on the Common Criteria security evaluation methodology [6]. This framework can be extended to other CPS applications such as health management and traffic control. Further, we expect that our work is beneficial for secure delivery of software to electronic control units (ECUs) of automobiles [7].

In the next two sections, we present the proposed security framework for the aerospace CPS, important challenges, and research problems. In Section IV, we consider extending the framework to automotive CPS.

II. SECURE AEROSPACE CPS SOFTWARE AND DATA DISTRIBUTION

Fig. 1 shows a generic system model that distributes aerospace CPS assets, i.e., loadable software and data, called Airplane Assets Distribution System (AADS). The suppliers assuredly design and develop loadable

Any findings, conclusions or recommendations in this material are those of the authors, and should not be interpreted as of The Boeing Company.

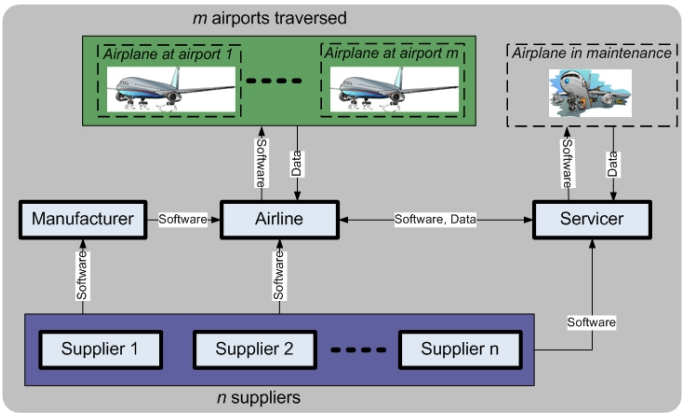

Fig. 1: Illustration of AADS model with a deployed airplane.

software as per safety standards such as RTCA DO-178B [8], and then distribute them to the airframe manufacturer or to the airline. The deployed airplane interacts with ground systems of its airline and/or of servicers contracted by the airline. Software and databases are delivered over the network by ground systems, and software is installed into a destination line replaceable unit (LRU) by maintenance personnel. The airplane configuration report must be distributed to ground systems to ensure successful software upload.

The adversary in the AADS attempts to actively attack CPS assets during their distribution, incurring unwarranted flight delays and lowering safety margins. For example, inserting/deleting software to create incorrect airplane configuration, or corrupting assets to delay/evade their detection.

The objective of the AADS is to securely distribute CPS assets end-to-end, i.e., from the source to the intended destination, in the presence of the adversary. Enabling the AADS to meet this objective is non-trivial, given the system's large-scale, distributed and complex nature. In [3], we have specified security requirements and analyzed that high assurance is needed for the integrity and authenticity of the distributed safety-critical assets, e.g., DO-178B Level A-C assets [8]. Our proposed solution approach makes use of digital signatures and certificates for protecting assets [3].

III. Relevant Challenges & Open Problems

The following fundamental challenges and open problems emerge in the proposed approach.

- *Providing key and certificate management*: The use of digital signatures mandates the integration of mechanisms and processes that can manage keys and certificates in the AADS. However, factors such as global traversed paths of airplane, lack of guaranteed network connectivity, multiple connecting ground stations and applications, lifetime of CPS assets, and airline cost constraints, complicate the design of suitable solutions for managing airplane private keys as well as certificates for validating received assets and airborne/ground entities in the AADS [5].
- *Achieving high assurance for a complex system*: To enable the useful and secure integration of the AADS for CPS asset distribution and other critical aviation applications, high confidence in the end-to-end security properties is needed. However, factors such as multiple entities involved and the complex interaction between components at an entity, make establishment of a high level of confidence a major challenge.
- *Strengthening secure software distribution*: Despite securing the end-to-end distribution, there are vulnerabilities, e.g., CRC check of received software at the LRU and compatibility conditions of software, as well as management and use of airplane configuration report, which may be exploited by the adversary in the AADS. Such vulnerabilities and weaknesses require further mitigation controls and mechanisms.

The above challenges translate into major research problems such as the following.

- *Design of PKI for the AADS*: Currently available public key infrastructure (PKI) are evaluated at a medium assurance level, e.g., at CC evaluation assurance level EAL4 [6]. The AADS, however, would require design and development of a PKI certified at high assurance levels. In addition, the PKI must support global operation of airlines and interoperability between AADS entities.
- *Use of formal methods for end-to-end analysis of the AADS*: Formal methods (FM) offers a technique towards providing high assurance for the design and development AADS. However, the cost and time efficient use of FM for end-to-end evaluation of large and complex systems is a challenging problem. A potential solution approach is to focus application of formal methods to only the critical AADS components.
- *Removing vulnerabilities in the AADS*: The installation of software must be made robust by (*i*) ensuring that the version and intended destination of the software can be verified, and (*ii*) ensuring the airplane software configuration report is securely delivered to ground systems and is validated. Further, adequate hardware and/or software redundancy is required to tolerate failures from execution of corrupt software that passed CRC check at some LRU.
- *Analyzing impact of security on safety*: While it is clear that security affects safety, it is not clear how

to present security requirements and functions in the context of a safety analysis. Since impact of security threats can evolve, the traditional quantitative and probabilistic safety analysis techniques become inapplicable for security evaluation. Therefore, new approaches are needed to integrate the discrete security evaluation methods into safety analysis [3].

IV. Challenges in Automotive CPS Software Distribution

The delivery of software and data to embedded electronic control units in deployed automotive CPS, i.e., intelligent vehicle, is an emerging problem [7]. Automotive software updates are often needed to patch up bugs in code or when vehicle user has subscribed to value-added services such as navigation.

To a large-extent, the software distribution system model can be considered the same as the AADS, with the vehicle user replacing the airline and with additional entities such as content providers who offer the value-added services to the vehicle user [7], [9]. Consequently, the challenges and problems discussed in the previous section can also fundamentally apply to the automotive CPS. However, unique features exist in the automotive CPS that give rise to new challenges as discussed next.

Unlike airlines, the vehicle user cannot be expected to be responsible for delivering and installing software updates or for maintaining correct software configuration. This complicates the secure and timely installation of software updates onboard vehicle. Further, unlike the airplane where physical and logical security controls are implemented to restrict onboard access, the vehicle is more accessible locally to attackers. Hence, in addition to secure software distribution and installation, vehicles require trusted computing and storage for protecting installed software [9].

Furthermore, while the traversed paths of vehicles do not scale globally, the number of deployed vehicles is relatively large. This scalability requirement presents unique PKI challenges, including key and certificate management. Moreover, certificate management is further complicated by change of ownership which can be expected to be more frequent for automotive CPS.

Additionally, group based solutions become more desirable for scalable secure distribution to many vehicles [4]. However, at the same time, value-added services warrant the need for confidentiality and access control for some software/data distribution.

V. Conclusions

In this paper, we considered the future eEnabled airplane to be an aerospace CPS and overviewed our work on the secure distribution of software and data of the aerospace CPS. We discussed major challenges and problems that remain to be addressed. We considered extensibility of our work on the aerospace CPS to the intelligent vehicle as an automotive CPS, and showed that innovations for high confidence establishment can mutually benefit both CPS.

References

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

[2] K. Sampigethaya, R. Poovendran, L. Bushnell, Security of Future eEnabled Aircraft Ad hoc Networks, to appear in *Proc. of AIAA ATIO*, 2008.

[3] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, J. Bußer, J. Cuellar, Electronic Distribution of Airplane Software and the Impact of Information Security on Airplane Safety. Proc. of Safecomp, 2007.

[4] K. Sampigethaya, M. Li, L. Huang, R. Poovendran, AMOEBA: Robust Location Privacy Scheme for VANET, *IEEE JSAC*, October 2007.

[5] R. Robinson, M. Li, S. Lintelman, K. Sampigethaya, R. Poovendran, D. von Oheimb, J. Bußer, Impact of Public Key Enabled Applications on the Operation and Maintenance of Commercial Airplanes. *Proc. of AIAA ATIO*, 2007.

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

[7] A. Adelsbach, U. Huber, A. Sadeghi, C. Stüble, Embedding Trust into Cars - Secure Software Delivery and Installation, *Proc. of ESCAR*, 2005.

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

[9] M. Wolf, Embedded Systems: Trusted Computing for Automobiles, Trusted Computing Workshop, 2007.

[10] 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, 2007.

Scott Lintelman is the Information Assurance (IA) manager at Boeing Networked Systems Technology, responsible for setting Boeing's IA research strategy. *Krishna Sampigethaya*, *Mingyan Li* and *Richard Robinson* lead the security effort of the Boeing Phantom Works IA group. The IA team has a long-standing partnership with Boeing Commercial Airplane. *Radha Poovendran* is an Associate Professor in EE department at the University of Washington and founding director of the Network Security Lab (NSL). He has received many awards for his research contributions to energy-efficient wireless sensor routing and security, including NSF CAREER, ARO YIP, ONR YIP, PECASE.