Secure Aircraft Data Network (SADN) Cyber Security Research Plans

Kevin Harnett
Program Manager
Center for Cyber Protection
Volpe National Transportation System Center
RITA, US DOT
Cambridge, MA 02142-1093

Background

New designs for the Aircraft Data Network (ADN) and the use of new communication paths to aircraft (Internet Protocol, broadband and 802.11) will be implemented in next-generation (e.g. Boeing 787, Airbus 380) and legacy civilian and military aircraft. These enhancements will provide improved essential capabilities but will introduce new cyber security vulnerabilities that may jeopardize the safety of flight of aircraft.

In October 2005, the US Department of Transportation's (DOT) Volpe National Transportation Systems Center was tasked by the National Aeronautics and Space Administration (NASA) Glenn Research Center (GRC) Secure Aircraft System for Information Flow (SASIF) Program to develop a baseline of the cyber security requirements for a Secure Aircraft Data Network (SADN) on next generation civilian aircraft and provide Research and Development (R&D) recommendations to leverage related ADN programs. In February 20606, Volpe developed a report titled*„ "SADN Cyber Security Research Plans"*, which identifies the key areas of required cyber security R&D for next-generation ADNs.

In September 2006, the Volpe Center is supporting a follow-on effort with the US Air Force in support of the Airborne Network (AN) Program. There are security concerns and problems that are common to both civilian and military Commercial Derivative Aircraft (CDA) ADNs that will require R&D. A Vulnerability Assessment study is being conducted by the Volpe Center to identify the areas of joint cyber security R&D for both civilian and military aircraft.

Overview

Plans for extensive modifications to the next generation of Aircraft Data Networks (ADNs) and an expansion of external network connections to provide enhanced communications form the ground to the aircraft are currently in progress. These changes introduce new cyber security vulnerabilities to aircraft that formerly have not been an issue of concern. If not properly mitigated, these vulnerabilities can expose mission critical aircraft control systems to malicious attack and infection by viruses, and result in unsafe flight conditions. To avoid the possibility of unsafe flight conditions, it will be necessary to perform a variety R&D projects to provide assurances of the implementation of a Secure Aircraft Data Network (SADN).

Future Boeing and Airbus ADN Plans

Boeing is developing a next generation commercial aircraft, Boeing 787, which will be certified in 2008. Airbus is in the final stages of certification of the Airbus 380, which is due to be operational in 2006. Both of these new commercial aircraft will implement the new ADN and communications capabilities. The new ADNs will make use of emerging technology to provide cost effective operating efficiencies and needed new revenue opportunities for aircraft operators, provide for desirable new services for aircraft passengers and enable state-of-the-art information sharing required for modern military operations. The new ADN will also have inherent cyber security vulnerabilities that have the potential to introduce safety of flight problems.

Legacy ADNs

Prior to the implementation of the next generation ADN, mission critical systems on the aircraft have been isolated from the outside world. Changes to critical systems have been made under tight physical security controls. Communications between the ground and the aircraft have been limited and controlled. With the advent of ADN, mission critical systems will be part of an integrated physical network that will include airline service systems, in-flight entertainment (IFE) systems and wireless access points that will accept connections from passenger owned devices. The connection of ground data networks to critical functions

in the ADN will be expanded to include external connections (both wired and wireless), using private and potentially public IP addresses. The aircraft will potentially become susceptible to the same cyber attacks as terrestrial-based systems (such as web sites, e-business applications and home computers) and will be a likely and alluring target for terrorists, cyber criminals and hackers.

Related ADN Programs

In addition to the manufacture of the Boeing 787 and the Airbus 380, there are a significant number of other projects and activities underway by stakeholders within the government and private industry that relate to the ADN. Airline operators, such as United Airlines, are making plans to implement elements of the new ADN and communications modifications (e.g. wireless LANs) in their existing fleets (e.g. B-747, B-737), that will add new cyber security vulnerabilities and SADN challenges. ARINC/Airlines Electronic Engineering Committee (AEEC) subcommittee on Security (SEC) are working to define ADN security standards and internationally, the European Organization for Civil Aviation Equipment (EUROCAE) WG-72, Aeronautical Information System Security, is also working towards the definition of ADN security requirements. Within the FAA and NASA, there are several ADN-related projects such as the Software and Digital Systems Safety (SSDS) Security LAN Study, Automated Airborne Flight Alert System (AAFAS), and the Airborne Internet. The FAA's Joint Planning & Development Office (JPDO) has defined a vision in their Next Generation Air Transportation System (NGATS) plan that calls for the harmonization and integration of civilian and military operations. The DoD/DHS are working on next generation military aircraft concepts and infrastructure, such as the Global Information Grid (GIG), that will enable the shared situational awareness that will be essential to their mission.

Required SADN Certification Criteria

The airframe manufacturers and airline operators have done exceptional work in assuring the airworthiness and safety of aircraft. The certification of aircraft is supported by federal laws and FAA policies mandating the safety of aircraft. Aviation industry organizations such as the Radio Technical Commission for Aeronautics (RTCA), the Society of Automotive Engineers (SAE) and Aeronautical Radar, Inc. (ARINC) provide standards and detailed certification methodologies and criteria that describe the process for certification and the metrics to insure that the standards are met. Since Cyber security vulnerabilities have not previously been an impediment to the safety of flight, neither the federal laws, nor FAA policies, nor certification methodologies and criteria to address the effect of cyber security vulnerabilities on airworthiness and safety are in place.

The implementation of the ADN and evolving technology is moving at a faster pace than the capability of the FAA to effectively regulate it. Given the current status, it is unlikely that the FAA, DoD, and DHS can provide assurances that cyber security vulnerabilities will be mitigated in the operational ADNs. It will be necessary to insure that emerging policies, certification criteria and procedures will provide the necessary assurances that the vulnerability introduced by the new cyber security vulnerabilities has been mitigated to acceptable levels. The vulnerability mitigation will be dependent on the implementation of a comprehensive security architecture comprised of effective security controls.

Recommendation

There is, however, a lack of direction, oversight and coordination among the various programs from the Federal Government. A SADN Program to maximize the coordination of efforts, strategic partnering and leveraging of key accomplishments from these and other ADN-related programs should be initiated and managed. The government will need to conduct SADN R&D to achieve the necessary assurances and the development of certification criteria process and procedure for security.

About the Author

Kevin Harnett is a Program Manager for the United States Department of Transportation at the Volpe National Transportation Systems Center located in Cambridge, Massachusetts. Over the past nine years, Kevin has been responsible for providing technical leadership in planning, implementing and managing high priority programs involving Information System Security (ISS) and risk management for the Department of Transportation (DOT), Federal Aviation Administration (FAA), NASA, Department of Homeland Security, Transportation Security Administration, Coast Guard, and other agencies, with special emphasis on security risk management, security policy, security training, certification/accreditation, security awareness, security testing/evaluation, incident response capability and remediation

Mr. Harnett has over Twenty-five years of combined project management, technical consulting, and implementation skills. Areas of expertise include: information security, network security, risk management,

requirements analysis, systems analysis/development, system architecture, cost/benefit analysis, system development/testing/implementation, Relational Database Management Systems (RDBMS), Capability Maturity Model (CMM), Computer-aided Software Engineering (CASE) tools, Computer-aided Design/Manufacturing (CAD/CAM), automated authoring systems, and document imaging/document management systems.