Onboard Aviation Information Assurance

Ravi Pendse, Professor, Electrical and Computer Engineering
Wichita State University, ravi.pendse@wichita.edu

Kamesh Namuduri, Associate Professor, Department of Electrical Engineering, University of North Texas, kamesh.namuduri@unt.edu

Brent Holmes, Chief, Platform Connectivity Branch,
Air Force Research Laboratory, brent.holmes@rl.af.mil

Abstract

The aviation infrastructure forms an important component of the nation's critical infrastructure. By considering the issues involved in protecting the onboard aviation information in conjunction with the introduction of Internet access within an airplane, we propose to investigate the risks, vulnerabilities, and threats in providing network connectivity to airplanes and a comprehensive set of supplementary security mechanisms to address these issues.

The first objective of the proposed discussion is to develop security and fault-tolerance solutions to the existing air-ground communication systems. The second objective is to investigate, design, and develop off-board control methods that would enable the ground crew to override the on-board control mechanism in the event of malicious takeover of an airplane. These objectives will be achieved by investigating the following four specific aspects of onboard information assurance.

(1) Identifying the risks, vulnerabilities, and threats
(2) Methods for downloading onboard aircraft parameters
(3) Air-ground network security and performance, and
(3) Off-line control mechanisms

The most significant result of the proposed work is a set of guidelines and best practices for securing onboard aircraft information suitable for practical implementation. The proposed activities also open up avenues for greater collaboration between universities and aviation industry resulting in safety and security of our nation's aviation infrastructure.

Discussion

Figure 1 illustrates the constituents of the infrastructure currently employed by airplane manufacturers and/or operators to ensure seamless connectivity with the airplane from the ground [1]. An airplane communicates with the ground networks via a plethora of communication channels that range from AM channels to satellite links. The Aeronautical Telecommunication Network (ATN) Fixed Network (in Figure 1) is a typical infrastructured network currently in the prototyping phase employed by the Federal Aviation Administration (FAA) (in the US) for eventual deployment across the nation to provide connectivity between

various end-stations including data centers and communication consoles. The ATN is an integral part of the FAA Telecommunications Initiative (FTI) and is currently being employed as a carrier for the Air Traffic Services Message Handling System (AMHS).

With a growing emphasis on the security of critical national infrastructures, the research community has turned its attention towards safe-guarding the national aviation infrastructure from potential malicious cyber attacks. We propose a set of supplementary security mechanisms that would enhance the currently available aviation security framework in an effort to circumvent most of the issues related to the deployment of an ATN.

Providing network connectivity to the airplane facilitates download of the onboard aircraft parameters to the ground stations periodically. We envision three different networks within the airplane. The Passenger Network (PN) is used by passengers within the airplane to access network resources on the global Internet. The Crew Network (CrN), on the other hand, is meant for the crew of the airplane to access resources not only on the global Internet, but also to access resources within the airplane's home network. The Control Network (CoN) is a strictly regulated network wherein the various components of an airplane interact with each other. As such, only authorized personnel are allowed access to the CoN. In order to maintain the separation among the three networks, we can consider having three physically separate networks. Tripling the network infrastructure is not a practically feasible solution. The alternative is to develop a Virtual Local Area Network (VLAN) based solution on a single network.

The primary driver for the adoption of the VLAN approach stems from the fact that the three networks utilize a common link (that is, a satellite link) to communicate with their corresponding home networks. By employing different VLANs for different networks within the airplane, the economics, performance and security features of a networked airplane could be administered in an efficient manner. The deployment of a VLAN based network within the airplane necessitates careful consideration of the various security threats that could hamper the operation of these networks.

Another solution that needs investigation is a thin client model for passenger network. In thin client model, the clients will not be running any applications. Instead, only screen updates would be sent over the air eliminating or isolating some threats.

An integrated security framework requires a careful consideration of the security features of the network within an airplane. Security mechanisms that are valid for terrestrial networks need to be enhanced for their integration into the framework of aviation security since the non-availability of the link connecting the airplane with its ground stations could potentially result in loss of revenue. At the network level, IPSec provides security to packets flowing between IPSec peers. The use of Mobile IP within the framework of a networked airplane necessitates the deployment of several security enhancing features of Mobile IP.

The presence of network connectivity between the airplane and its ground stations presents numerous challenges in terms of security provisioning. Unlike terrestrial networks, the network connecting an airplane with its ground stations cannot sustain outages as this would result in not only considerable loss of revenue. Therefore, the security provisioning within the IP network connecting the airplane with its ground stations needs to be carried out to ensure minimal, if any, network outages due to malicious network activity, both within and outside an airplane. There are numerous risks associated with the network connectivity solutions. For example, a hacker may go through the control system on the ground to take control of the aircraft. A hacker may

also plant a zombie that may execute at a set date and time. We should analyze on-board methods to enable the air crew to override a malicious take ove and restore the airplane to a normal state.

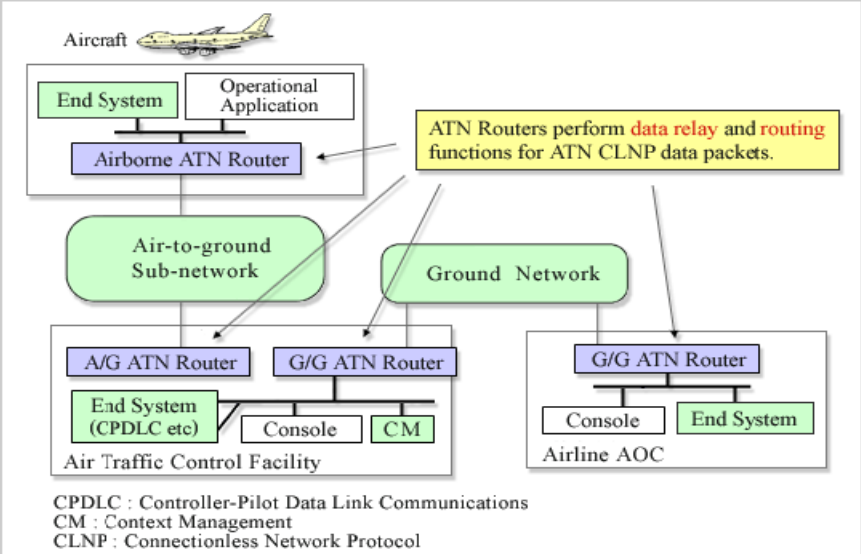

Figure 1: A typical networked airplane and the corresponding systems on the ground stations including Airlines Operations Center (AOC) and Air Traffic Control Facility [1].

Ravi Pendse has been with WSU since 1994. He is currently a full professor in the ECE department and a Wichita State CISCO fellow. He regularly teaches courses related to his core competencies: Routing and Switching, Multi-services over IP, and Storage Area Networks. At the university level, Pendse serves as the Chief Information Officer (CIO) and associate vice provost for academic affairs at WSU.

Namuduri is an Associate Professor the department of Electrical Engineering at the University of North Texas (UNT). His research interests include Information Assurance and Video Processing and Communications. He was the PI for the NSF funded Capacity Building project at Clark Atlanta University. At WSU, Namuduri took the leadership role in developing a comprehensive IAS curriculum at WSU and getting the curriculum approved by CNSS division of NSA as having met the 4011 and 4013 standards.

Brent Holmes is chief of the Platform Connectivity branch at the Air Force Research Laboratory, Information Directorate, Rome, N.Y. The Air Force Research Laboratory is the premier Air Force research organization leading the development of future Information Technology capabilities. Mr. Holmes leads the science and technology efforts for the discovery, development, and integration of innovative and affordable technologies that connect ground, air, space and cyberspace assets to deliver Air Force war fighting capabilities.

References

1. ATN router overview, www.oki.com/jp/SSC/ITS/eng/image/atn200303.pdf.