Aviation Data Networks: Security Issues and Network Architecture

N. Thantry

R. Pendse

Affiliation:
N. Thanthry and R. Pendse. Department of Electrical and Computer Engineering, Wichita State University, Wichita, KS

Aviation Data Networks: Security Issues and Network Architecture

N. Thanthry & R. Pendse
Wichita State University

ABSTRACT

The Information Technology (IT) revolution, combined with people's need to access information quickly, has resulted in the explosive growth of the Internet in the past decade. Ubiquitous access to the Internet has become an essential component of a mobile workforce, and multiple mechanisms are being devised to ensure seamless connectivity to corporate resources. An integrated security framework requires careful consideration of the security features of the network within an airplane. Potentially, the aircraft could consist of three kinds of networks, namely: passenger network, crew network, and control network. The security protocol implemented must ensure a proper separation of these networks and also watch for any security protocol violations. In this paper, the authors review existing aircraft data network standards, security provisioning, and security threats associated with the aircraft data networks. In addition, the authors also analyze the security threats associated with different network architectures.

INTRODUCTION

Over the past decade, there has been a tremendous growth in the communication field. Internet usage has grown beyond all expectations. This development has led to technological growth in the wireless networking field. Wireless Internet access and protocol development have prompted users to opt for mobile devices to access the Internet. At the same time, aircraft communications have become significantly innovative. From initial communication systems that were based on radio technology and mainly used for communication between the pilot and the ground station, today's aircrafts use satellite-based communication systems that could be used for advanced flight control and passenger benefits. The current broadband communication systems (satellite communication systems) provide a bandwidth on the order of 8 to 10 Mbps. With the availability of bandwidth and the help of technological growth in the mobile Internet access field, the airline industry is moving toward providing data network access to its passengers.

Communication networks within airplanes introduce many new possibilities. Along with providing Internet access to passengers, a communication network could also be used to enhance flight safety and flight control. Some airplane manufacturers have gone one step further and are planning to use data networks to connect flight components [1]. While this enables an easier control system, it involves some possible security and safety issues.

In this paper, the authors review existing standards related to aircraft data networks, security requirements, and security threats. They also explore security issues associated with various network architectures that could be used in aircraft data networks. Possible safety/security enhancement features that could be introduced within the airplane using Internet connectivity are also discussed.

The remainder of this paper is organized as follows: In Section II, the authors review various research efforts carried out in this area. In Section III, the authors discuss security requirements of aircraft data networks. In Section IV, the authors present a discussion of network architecture in view of aircraft security. In Section V, the authors present possible flight safety enhancement opportunities associated with Internet connectivity within the aircraft. In Section VI (the last section), the authors present their conclusions and future work.

RELATED WORK

Since the early 1970s, data networks have played an important role in avionics. In the primitive stage, an aircraft consisted of federated systems (defined by ARINC 429 [2] standard), where each flight component was operating with its own set of software/hardware components. Different flight components were connected using point-to-point links. While this implementation was functional, it had limitations in terms of available bandwidth and the number of connections, as most of the connections were point-to-point (rarely point-

to-multipoint). In addition, ARINC 429 was incompatible with commercial off-the-shelf (COTS) equipment. As the need for bandwidth and data dependency between different flight components grew, the aircraft industry was compelled to adopt new ways of connecting these different components.

In the early 1990s, an integrated subsystem (ARINC 629) was introduced in aircrafts [2]. In the integrated subsystem, some Line Replaceable Units (LRUs) were connected to a common data bus. However, different modules were still connected using the ARINC 429 standard. One of the main improvements that ARINC 629 achieved was in terms of redundancy requirements. While ARINC 429 required component-level redundancy, ARINC 629 improved it by defining module-level redundancy. It was observed that ARINC 629 was expensive to implement and incompatible with COTS equipment, just as the case with ARINC 429. In addition, it was observed that integrated subsystems were effective only for small amounts of data transfer. This led to the development of the ARINC 664 standard that defines total system integration.

The main purpose of ARINC 664 was to identify commercial standards that could be used in avionics with little or no modifications. One of the main goals of ARINC 664 was to establish a connection between various networks that could be situated within an airborne airplane. It began with IEEE 802.3 (Ethernet) standard and RFC 1122. Based on the IEEE 802.3 standard, ARINC 664 defines a single data bus that connects various flight components within the aircraft. The commercial standards adopted within ARINC 664 enable multiple networks with different characteristics to co-exist within the airplane. In addition, ARINC 664 enables the use of COTS equipment in the design and broadly divides the networks within the airplane into four different groups: flight deck, OEM, airline, and passenger that are based primarily on their determinism requirements. Part 5 of ARINC 664 standard addresses security issues associated with aircraft data networks. It specifies using IPSec-based encryption, key exchange, and authentication schemes to ensure network security. In addition to using cryptographic methods, the standard also suggests employing packet filters, application level proxies, and circuit-level gateways to ensure security within the airplane.

In addition to ARINC 664, some additional standards are generally used while designing an aircraft network. ARINC 628 defines the cabin equipment interfaces. ARINC 746 defines the cabin communication systems. The aviation satellite communications system is defined in ARINC 761, and the network server system is defined in ARINC 763. The network architecture and components used to design an aircraft network should comply with all of the above standards, and meet safety and security requirements.

Along with ARINC standards, various other research publications discuss aviation security requirements. Most of these publications concern application security and IPSec-based encryption mechanisms to improve security. However, in aviation data networks, security should be considered in a different perspective. As stated in ARINC 664-part 5, network security (security of the network layer including the link layer) is more important than application security.

Apart from the ARINC standards, other research efforts have concentrated on enabling mobility support protocol (mobile IP) and multimedia applications within the airplane. Kent Leung et al. in their technical report to NASA [3], suggested that the aircraft data network could use either a LEO or GEO satellite system for external world connectivity. Ronga et al. [4] proposed a framework to support multimedia applications over satellite links in view of the aircraft telecommunication network.

Tingey and Parkinson [5] discussed prospects for the development of secure avionic network applications using TCP/IP. They suggested using the VxWorks-based IPSec implementation for a reliable avionics network. Franzrahe [6] identified certain safety features that could be enabled with data networks within an airplane. In their technical report, the authors suggested that Internet connectivity could be used for real-time surveillance of the aircraft. They also observed that Internet connectivity could be used to assess the flight status in real-time rather than waiting until the pilot communicates with the controlling station.

In this paper, the authors concentrate primarily on the network security aspect of aviation data networks. In the next section, the authors discuss various security issues associated with aviation data networks.

AVIATION SECURITY REQUIREMENTS

Along with safety, the avionics subsystem must also possess sufficient security provisioning for successful deployment. In a recent report, the United States General Accounting Office warned that while the extent and effects of cyber terrorism on US infrastructure has not been determined, aviation and other key infrastructure installations are highly vulnerable because of their indivisibility from global communication [7]. Adoption of open standards for data networks has further increased security concerns. In addition, care must be taken about security requirements while achieving interoperability between various systems within the airplane.

Any network system must address three basic security requirements: confidentiality, authentication, and integrity. Data confidentiality ensures the privacy of the end users and protects their data from spoofing. Similarly, data integrity ensures that the data sent by the end user is not modified by any malicious element in the network. Authentication is one of the most important factors in network security since it controls access to network resources and ensures that only valid users have access to network resources.

In addition to the above requirements, an airplane network needs additional security in terms of separation between various network segments. The control network must be protected from unauthorized access, which requires that it be separated from the passenger network. Also, usage of the passenger network resource must be monitored and controlled (if necessary), which requires that it be connected to a gateway

that performs both monitoring and controlling functions in addition to providing Internet access.

SECURITY ISSUES

The security issues involved with airplane networks can be broadly classified into two categories: external and internal.

External security issues are primarily related to the external link connecting the airplane network to the ground station and to the protocol used to provide mobility support. This network could be connected to the ground station by either satellite links or wireless links, depending on the location of the airplane. While the airplane is airborne, it could use satellite links to establish connectivity with the ground station. If the airplane is within the range of a wireless access point, it could even use wireless media to connect to the external world. Each of these media has associated security concerns. Recent studies [8, 9] have shown that IP over a satellite link is not very secure and suggest using encryption (preferably IPSec encryption) in order to protect data. Similarly, wireless networks are also prone to security threats. Significant research efforts have been undertaken to improve the security of wireless links. Wired equivalent privacy (WEP) [10] is one of the most widely used security mechanisms for wireless networks.

Along with addressing the security concerns of external links, these protocols also address security issues related to the mobility support protocol. Mobile IP [11, 12], one of the most widely accepted mobility support protocols, does not define any security mechanisms to protect mobile device data. Many researchers have suggested using IPSec encryption along with Mobile IP [13, 14] to achieve data security. In addition, IPSec could also be used for authentication purposes.

Compared to external threats, more severe security threats could originate from within the airplane. With the co-existence of passenger and control networks, the control network could be exposed to attacks from the passenger network, either in the form of denial of service [15] or an access violation. Any security breach with the control network may result in serious consequences to flight safety. Hence, it is very important that the architecture design provide a proper separation between the control network and the passenger network.

NETWORK ARCHITECTURE

In the previous section, the authors presented various security issues involved with aircraft data network design. In this section, some possible network architectures, and their properties, within the aircraft are discussed.

Avionics Subsystem Design

The main requirements of the avionics subsystem are high determinism and low response time. Different layer two technologies, such as Ethernet, ATM, Fibre Channel, and InfiniBand, could be considered to provide both requirements. Ethernet is one of the strongest contenders for connections between various flight subsystems and is also mentioned in ARINC 664 standard.

The wide usage of Ethernet, with its COTS components, equipment and software availability, and independence from network topology, makes it the most attractive choice. However, a recent study [16] that compared Fibre Channel, ATM, and Ethernet technologies demonstrated that ATM might be a better choice over the other two, since it could be used in local areas as well as wide-area networks. In addition, ATM can also operate over satellite links, which makes it more flexible. However, another study [17] indicated that InfiniBand might be the best fit for future avionics communications. InfiniBand reduces the complexity of the computer processing system in addition to providing high bandwidth. InfiniBand switch fabric also provides both partitioning and QoS at each switch port to manage performance levels.

Avionics Data Network Design

Security and quality of service are two important parameters that must be considered when designing aviation data networks. The quality of service here does not reflect the quality of service requirements of the end-user applications, but it represents the requirements of the avionics subsystem itself.

One of the major security requirements of aviation data networks is the separation of different network subsystems. An aviation data network could possibly contain three major network segments, namely a control network, crew network, and passenger network. As the names suggest, the control network predominantly consists of avionics components, the crew network is used by the flight crew for monitoring purposes, and the passenger network enables Internet connectivity for passengers.

In order to protect the control network from unauthorized access and security attacks, the control network must be separated from the rest of the aviation data networks, either logically or physically. In the case of logical separation, the control network, the crew network, and the passenger network could all be connected to the same Ethernet switch, as shown in Figure 1. The three networks are separated using VLANs. While VLANs provide a very basic form of security for individual network segments, they are prone to security attacks [18]. The most common attacks experienced by the VLANs are shown in Figure 1.

- *MAC Flooding Attack:* Each switch has a limited amount of memory to store the identities of devices connected to it. When the memory becomes full, the new addresses will not be stored and the packets belonging to these new addresses will be flooded. An attacker could use this weakness to turn the switch into a dumb pseudo hub and sniff the traffic flowing through the switch.

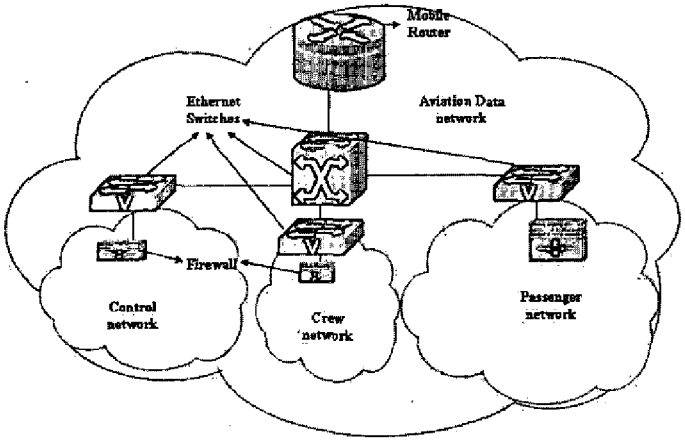

Fig. 1. Network scenario with switched Ethernet connecting control, crew, and passenger networks

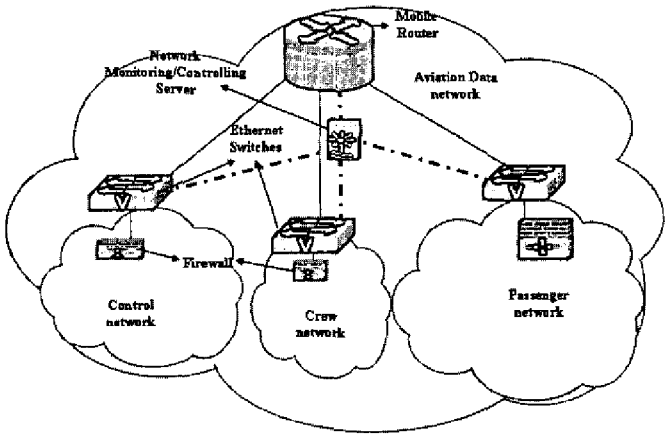

Fig. 2. Separation of control, crew, and passenger networks using multiple interfaces at the mobile router

- *802.1Q and ISL Tagging Attack:* Tagging attacks allow a user on a VLAN to get unauthorized access to another VLAN. This occurs generally when a port in the switch is configured DTP auto, and it receives fake DTP packets. In the event that it receives fake DTP packets, it acts as a trunk port and starts accepting packets to any VLAN. Using this compromised port, a malicious user can access other VLANs.

- *Double-Encapsulated 802.1Q/Nested VLAN Attack:* This form of attack is used to transmit packets from one VLAN to another VLAN without proper authorization.

- *ARP Attack*: This is one of the oldest forms of attack, where a malicious user claims the ownership of an IP address associated with a different MAC address by changing his/her own MAC address.

- *Multicast Brute Force Attack:* This attack tries to exploit switch vulnerabilities against L2 multicast frames.

- *Spanning-Tree Attack:* This attack also tries to exploit the bugs/weaknesses in the switch.

- *Random Frame Stress Attack:* In this form of attack, a malicious user varies different fields of the packet, keeping the source and destination addresses the same. In this way, the attacker tries to transmit the packets across VLANs.

In the case of physical separation, the control network, the crew network, and the passenger network are configured as three separate mobile networks. The mobile router, which provides external world connectivity to the airplane, will have multiple interfaces – one for each network type. This network configuration is shown in Figure 2.

The physical separation provides better security than VLAN-based connectivity because the networks are separated by a router. This reduces the possibility of any sniffing or eavesdropping. Also, the router can be configured as an additional firewall to stop all unwanted traffic from entering the control network.

While physical separation ensures a higher level of protection for the control network, it does not protect the control network from other security risks. The control network will still be prone to DoS attacks and unauthorized access attacks. These could be addressed by deploying a suitable firewall, as stated in the ARINC 664 standard.

Network Activity Monitoring Tool

Selection and placement of network activity monitoring tools play an important role in aviation data network security. The ARINC 664 standard suggests using proxy servers to improve both performance and security. This standard also mentions placing packet filters in strategic locations to further protect the aviation data network from external/internal attacks. In addition to these proxy servers and packet filters, using a dedicated network activity monitoring/controlling server would help improve security.

The network activity monitoring/controlling server could be built in line with an intrusion detection system (IDS). However, unlike normal IDS, the network activity monitoring/controlling server can make decisions based on the data feed from many sources, including the cabin voice recorder and surveillance equipment placed at strategic locations within the airplane. The server could potentially control all the active forwarding devices. Depending upon network activity and security status of the aviation data

network, the server can reconfigure the active devices and facilitate control network traffic during emergency situations.

POSSIBLE SAFETY / SECURITY ENHANCEMENT FEATURES

Providing Internet access to airplanes when they are airborne enables the introduction of new features within the flight. Some of these features are related to flight safety/security and some are commercial in nature. A list of possible supplementary flight safety/security features that can be deployed in an Internet-enabled airplane follow:

- *Download of Flight Critical Data in Real-time:* The black box plays an important role in retrieving important data from a crashed airplane. A black box contains two parts: a cockpit voice recorder (CVR) and a flight data recorder (FDR). As the name suggests, the CVR unit records the voice activity inside the cockpit, and the FDR records vital data (such as flight speed, altitude, temperature) related to the flight. Most black boxes used in today's airplanes are either made of magnetic tapes or solid-state memory boards. Magnetic tape-based black boxes are being phased out, and most black box manufacturers are opting for black boxes with solid-state memory boards, which can accommodate up to two hours of audio data and 25 hours of flight data.

One of the main drawbacks of the current implementation is that information retrieval is not real-time. The possible delay in retrieving the black box may result in some or complete data loss. With existing computer hardware technology, it is possible to use a high-capacity storage device within an airplane. This device can be connected to a server and also to a traditional black box/sensor network. One of the main advantages of using a server with a storage device is that the server can mirror all the flight data to the ground station in real-time using available Internet connectivity. This enables the ground station to monitor the flight status/health and assists the flight crew in disaster situations.

- *Real-Time Video Surveillance:* Flight safety/security is one of the most widely discussed topics in the aviation industry today. The US government is trying to find every possible option for providing secure flights for passengers. Following the 9/11 incident, most airplane manufacturers and passenger flight service providers are insisting on using surveillance equipment to ensure flight safety. Many commercial aircrafts have already deployed, or plan to deploy, video monitoring systems that will monitor the cockpit entrance as well as the passenger section of an airplane. Currently, the video is displayed on a LCD monitor and also stored in a server [19] within the airplane. While this ensures better security, it does not assist the ground station authorities in assessing the situation during disastrous events.

Existing video compression standards make it possible to transmit video signals to the ground station in real-time, thus enabling the ground station to monitor in-flight activities during abnormal situations and to make appropriate decisions. This also helps the ground crew prepare for medical emergencies.

- *Remote Controlling:* In situations where the flight crew is compromised or is unable to control the flight due to unforeseen circumstances, the ground station could enable remote controlling of the airplane for safe landing.

- *Flight Location Tracking:* It is very important for authorities to monitor the location of an airborne airplane. Typically, air traffic control keeps track of the flight location using transponders that detect a radio signal from the air route traffic control center or terminal radar control center and responds with an amplified signal specifying crucial flight data, including flight speed and height information. Although this system works efficiently, it is possible to turn off the transponder with the existing implementation. This poses serious security threats to flight safety/security.

The mobile router used to provide internet access to the airplane can also be used to track the airplane's position. The mobile router must register (a requirement of the mobility support protocol) with both the foreign agent (attached to the satellite network) and the home agent (attached to the ground station) when the airplane is moving. In most cases, the path of the airplane will be predetermined. Using this and the mobile IP feature (registration), flight movement can be monitored.

Apart from these applications, many other applications could be enabled using Internet connectivity. Some are related to flight security, while others to enhanced flight services. These applications need certain infrastructure support in terms of security and quality of service for successful deployment.

CONCLUSIONS

Data network-enabled aircrafts have opened up a new set of service opportunities. At the same time, they have also introduced several security threats that must be addressed. These security threats can originate from outside the airplane or from within the airplane. Encryption mechanisms could address the security concerns related to external attacks. However, internal security threats can only be addressed by

choosing proper network architecture. In this paper, the authors analyzed the drawbacks of using switched VLANs for connecting various network segments within aviation data networks. They suggest using physical separation rather than logical separation to connect different network segments. In addition, they recommend using a network activity monitoring tool that could also control all active connecting devices and facilitate a safe and secure communication.

Currently, the researchers of the Advanced Networking Research Center (ANRC) at Wichita State University are investigating the feasibility of some of these proposed safety/security enhancements. A test network, similar to the airplane data network, is set up in the ANRC lab. The researchers are simulating both multimedia and normal data traffic transmission, similar to aircraft data network, and monitoring the performance and security issues associated with transmission. The researchers are also working on a mechanism to securely transmit critical flight data to the ground station without affecting performance.

ACKNOWLEDGEMENT

This research work is partially funded by the Cisco Systems, Cessna Aircraft Company, and the State of Kansas.

REFERENCES

[1] D. Braid, D. Jenson and C. Johnson,
Advanced Network Communications and Processing Architectures for Avionics Applications,
In the Proceedings of 6th Joint FAA/DoD/NASA Aging Aircraft Conference, September16-19, 2002.

[2] Airline Electronic Engineering Committee/ ARINC Standards,
http://www.arinc.com/aeec/draft_documents/.

[3] K. Leung, D. Shell, W.D. Ivancic, D.H. Stewart, T.L. Bell and B.A. Kachmar,
Application of Mobile-ip to Space and Aeronautical Networks,
Technical Report E-12548
(NASA TM-2001-210590), December 2001.

[4] L.S. Ronga, R. Fantacci, T. Pecorella and F. Volpi,
Real-Time QoS DiffServ Gateway Implementation for Satellite IP Networks,
COST 272 TD-02-013-P.

[5] P. Tingey and P. Parkinson,
Secure Networking for Avionics Systems,
pp. 81-85, Defense Procurement Analysis, Summer 2003.

[6] Franzrahe, M. De Sanctis and S. Tudge,
WirelessCabin – Market Survey and Recommendations,
Technical Report, IST-2001-37466 WirelessCabin-D5,
August 2003.

[7] Cybersecurity for Critical Infrastructure Protection,
Highlights of GAO-04-321, May 2004.

[8] M. Medawar,
Satellite Security: The Weakest Link?,
White Paper, GSEC Practical Assignment,
Version: 1.4b, SANS Institute 2003.

[9] Critical Infrastructure Protection – Commercial Satellite Security Should Be More Fully Addressed,
Highlights of GAO-02-781, a report to the Ranking Minority Member, Permanent Subcommittee on Investigations,
Committee on Governmental Affairs,
United States Senate, August 2002.

[10] N. Borisov, I. Goldberg and D. Wagner,
Intercepting mobile communications: The insecurity of 802.11,
7th Annual International Conference on Mobile Computing and Networking. July 16-21, 2001, Rome, Italy.

[11] C. Perkins,
IP Mobility Support for IPv4,
RFC 3220, http://www.ietf.org/rfc/rfc3220.txt.

[12] D. Stewart, D. Ivancic, T. Bell, B. Kachmar, K. Leung and D. Shell,
Application of Mobile Router to Military Communications,
in the Proceedings of MILCOM 1999.

[13] J. Binkley,
An Integrated IPSEC and Mobile-IP For FreeBSD,
Portland State University,
PSU Technical Report 01-10, October 2001.

[14] D. Khatavkar, E.R. Hixon and R. Pendse,
Quantizing the Throughput Reduction of IPSec with Mobile IP,
in the Proceedings of MWSCAS 2002.

[15] A. Hussain, J. Heidemann and C. Papadopoulos,
A Framework for Classifying Denial of Service Attacks,
in the Proceedings of SIGCOMM 2003, Karlsruhe, Germany.

[16] Network Technologies Investigation – NASA/GSFC High Speed Fiber Optics Test Bed,
Technical Report, http://misspiggy.gsfc.nasa.gov/tva/photonics/HiDataRate/index.htm.

[17] D. Riddel,
InfiniBand as an Avionics Net: A Proposal,
COTs Journal, October 2003.

[18] Virtual LAN Security Best Practices,
White Paper, Cisco Systems.
http://www.cisco.com/en/US/products/hw/switches/ps708/products_white_paper09186a008013159f.shtml.

[19] FlightVu,
CabinVu product data sheet, AD Airspace,
http://www.ad.aero.com/products_equipment.htm.