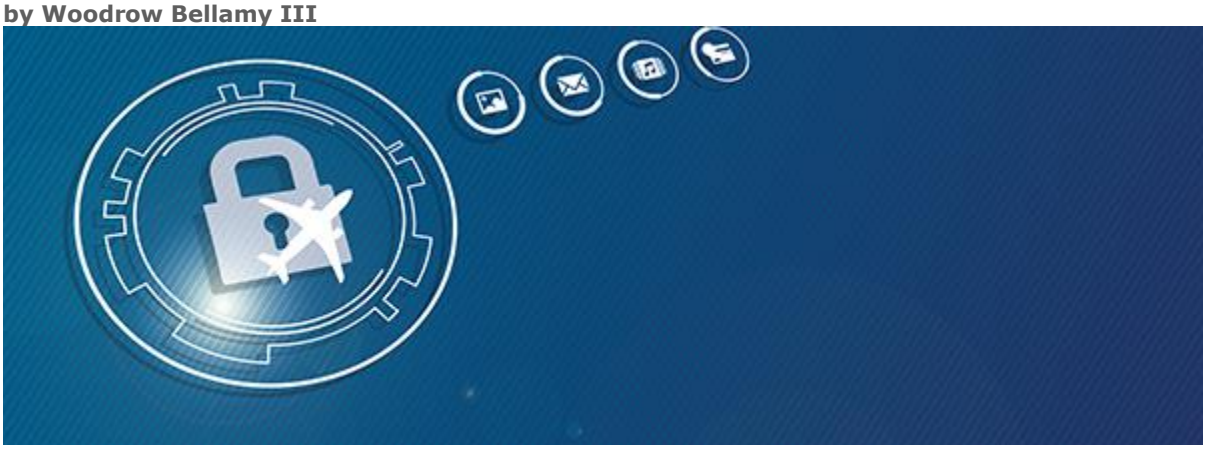
Monday, February 1, 2016

Aircraft Cyber Security Protection Scaling Up

As aircraft become increasingly e-enabled, the avionics industry is directly addressing the cyber security risks associated with Internet Protocol (IP) with new products, standards and federally regulated security protocols and methods.

by Woodrow Bellamy III



The Avionics Magazine aircraft cyber security Upgrade Central survey produced results showing 37 percent of readers that operate mostly fixed wing aircraft have needs to acquire new aircraft cyber security technology. In contrast, another 20 percent say they have upgraded their cyber security technology in the last 2 to 3 years and the remaining 42 percent do not need to acquire new aircraft cyber hardware or software.

Hardware

Cyber security risks associated with increasingly Internet Protocol (IP) connected aircraft became a global concern in 2015 after a Government Accountability Office (GAO) report raised concerns that the increased IP networking featured on modern aircraft has created a challenge with interconnectivity between cockpit avionics and cabin broadband networks. Firewalls are used to separate cockpit avionics from intrusion by cabin systems users, however the report states that because firewalls are software components, "they could be hacked like any other software and circumvented." That lead to a year of headlines and interviews with experts over what can be done to address those risks.

The risks are also difficult to analyze, as the experts at companies that manufacture cockpit avionics, cabin-based Wi-Fi and In-flight Entertainment (IFE) systems would rather not disclose how they prevent hackers such as Chris Roberts — who claimed to have accessed an aircraft's computer through its IFE system last year — from gaining access to critical flight control systems and attempting to alter the course of an aircraft path or perform some other malicious procedure. Roberts, the founder of security company One World Labs, was mentioned in a 2015 Federal Bureau of Investigations (FBI) affidavit last year after being able to access the Thrust Management Computer (TMC) through the IFE system of an unidentified Boeing aircraft. The affidavit claims Roberts was able to exploit the ARINC 429 data bus feed between the aircraft's navigation

systems that are used by IFE systems to populate animated maps on seat back screens and show the aircraft latitude, longitude and speed in moving map applications. Boeing released a public statement acknowledging this link, but also stated that the systems are isolated other than that one-way link and the architecture isolates them from other systems that perform critical and essential functions.

The top three reasons that respondents to our survey provided for wanting to acquire new aircraft cyber security technology, were: to improve the cyber security of an Electronic Flight Bag (EFB) platform; prevent potential hacker intrusion; and encrypt aircraft data exchanged with ground automation systems.

Thompson Aerospace CEO Mark Thompson says that the Irvine, Ca.-based provider of aircraft tracking virtual Flight Data Recorder (FDR) and secure data transfer products has a new system, the Connectivity Server Unit version 2 (CSUv2), designed to address all of the cyber claims featured in the 2015 GAO report associated with cyber risks on today's aircraft. CSU v2 has the processing, memory and I/O capabilities to enable a single part number to support all types of aircraft. The server has 2 QUAD core processors, each with 1,000 gigabytes of storage, to allow real-time processing and distribution of any ARINC, discrete, or other type of data to be sent over an Iridium link, wireless access point or LTE cellular network. But the real security comes into its dedication to hardware security engine duality and government security standards.

"The CSUV-2 has two local processors for the user to use. To do local processing it has a separate hardware security engine to control the aircraft systems and the local processing. This device has setup a methodology for a user so that when they log in they can have separate privileges and those privileges are determined by a login password and a piece of hardware the user has to carry with them, such as a USB device that they can plug into the system or a bluetooth device that he or she carriers along with him. With this, the user can log in and it has a secondary validation aside from just a user ID and a password," says Thompson.

With the CSUV2, Thompson also focused as much on verifying the source of data being communicated through aircraft avionics systems as they did on encrypting that data. In September 2015, the FAA released a new Advisory Circular 119-1 (AC 119-1) to describe an acceptable means of obtaining operational authorization for an aircraft certified with a special condition related to the security of the onboard computer network. Effectively, the AC provides guidance for developing an FAA-authorized Aircraft Network Security Program (ANSP) that directly addresses cyber risks, such as reduced performance, denial of service or overall criminal activity.

"Today what you do is you walk to the aircraft with a database and then on the [Flight Management Computer] FMC you type in a check board, which back in our youth we thought that was an acceptable means of doing security. The reality is that is not an acceptable means of doing security with the new paradigm. The Radio Technical Commission for Aeronautics (RTCA) has recommended in three documents to address the fact that the way we were doing security in the past is unacceptable and they made a requirement that all of the data has digital signatures," says Thompson, referring to RTCA documents DO-326A, DO-355 and DO-356, which combine to provide guidance on preventing unauthorized electronic interaction to aircraft safety, and tools used for performing an airworthiness security process.

Secure E-Enablement

Respondents to our reader survey on aircraft cyber security technology noted the leading reason why they would use or purchase aircraft cyber hardware or software products is to due to the increased use of IP on their aircraft.

In addition to products such as the CSUV2 available as post-purchase modifications, connectivity hardware recently approved for new aircraft such as Bombardier's C Series is also addressing cyber security risks. For example, the new Esterline CMC PilotView EFB and Aircraft Information Server (AIS), available as a factory option on the CSeries, provides an integrated information management system and network connectivity. The CSeries launch customer, Swiss International Air Lines, is the first operator to select the PilotView as a factory option on the CSeries, which Jean-Marie Begis, director of Esterline CMC's EFB and aircraft wireless systems product lines, told Avionics Magazine will be a secure e-enabled aircraft.

"The way you manage security is very complex, it's not a single protocol it's more a number of elements that allow us to gate or protect and filter traffic but also configure the system so that certain types of communications are allowed. There is a lot of procedural design involved as well, the way the systems are configured, modified and accessed in the aircraft," says Begis. "The AIS has all the pre-requisites to support network security, such as active firewalls, encryption support, application support and the likes, but it's more the complementary way we use them that is important in the configuration."

One of the biggest concerns that came out of the GAO's report on at-risk cockpit avionics systems, was the general notion that the broadband radio used for all Internet connectivity off of aircraft is shared by those controlling the critical functions in the front — pilots — and those surfing the web and watching Netflix in the cabin — passengers. Axel Jahn, managing director and vice president of business development for connectivity at Zodiac Inflight Innovations, says the company features cyber security within all of its RAVE aircraft connectivity and entertainment products.

"RAVE Cellular provides a mobile phone network on the aircraft. SITA OnAir is the network operator and its network has the same security features as a terrestrial mobile phone network. Through RAVE IFE, we provide IFE content either through the embedded IFE or wirelessly to passengers' own personal electronic devices. We use end-to-end encryption, based on widely accepted industry standards, to ensure the security of the content. This content protection is put in place in agreement with the studios, which own the content. RAVE Broadband is the hardware required to provide in-flight Internet access. The Internet Service Providers (ISPs) run portals over Zodiac Inflight Innovations servers. Our role, in terms of cyber security, is during the integration stage, when we analyze and test the security," says Jahn. "Technology for aircraft is typically several years behind what is happening on the ground. It takes time to develop and adapt the technology to make it suitable for the aircraft environment, both in terms of weight and size and, importantly, to ensure it does not jeopardize the safety of the aircraft. For example, we are currently working on the technology for 3G and 4G on aircraft. The result is that, by the time technology reaches the aircraft, any security issues have been addressed during terrestrial use."

Wind River was noted as the leading company for aircraft cyber security products used by respondents to the Avionics aircraft cyber security survey. Chip Downing, senior director of business development for aerospace and defense at Wind River, says its VxWorks Real-Time Operating System (RTOS) supports a secure Internet of Things (IoT) aircraft environment.

“Device manufacturers within the commercial aircraft segment face many challenges that can be addressed by taking advantage of IoT concepts. In order to operate aircraft within this space, manufacturers have to obtain an aircraft type certificate, which, in turn, means that devices within the aircraft have to be safety-certified, typically following the RTCA DO-178 and EUROCAE ED-12 standard for software, and RTCA DO-274 and EUROCAE ED-80 for hardware. These requirements mean that development of these devices is necessarily more complex than for similar consumer devices. But they can still benefit from the opportunity and efficiencies that IoT enables,” says Downing.

The company’s 2015 white paper, “The Internet of Things in Commercial Aviation,” advocates for the same aircraft cyber security concept proposed by the FAA in AC 119, noting that security should be addressed not only as part of the aircraft type certification but also as part of the ongoing airworthiness certification.

Thompson provides the best summation of addressing aircraft cyber security going forward for the industry. “The systems developed for aircraft need to hold the flexibility to allow the aircraft to be able to create keys based on who wants to view the data instead of just one key for all. You need a system that can deal with people who don’t have keys and people who do have keys and the system needs to be flexible to provide keys based on what level of security and authenticity you want to require for each user. I think that’s what the airlines and the OEMs need to focus on. Focus on what they do on the ground and mimic that in the aircraft,” says Thompson.

- See more at: http://www.aviationtoday.com/av/issue/departments/products/Aircraft-Cyber-Security-Protection-Scaling-Up_87179.html#.VwPZHKQrKUk