Securing Aircraft Becoming More Complex

Aviation Week & Space Technology

Bill Carey

Tue, 2018-06-05 04:10

Protecting aircraft from malicious acts is becoming more complex. Traditional security threats to aviation—hijackings, explosives, insider attacks—persist, but cybervulnerability of increasingly interconnected air and ground systems looms as a dominant future challenge.

A report underwritten by Thales and published by the Atlantic Council in November offers another take on the celebrated concept of the "connected" aircraft, one in which pilots can display real-time weather information on the flight deck, and passengers use the internet via cabin Wi-Fi systems. Maintainers using tablets can call up flight and maintenance data collected by onboard quick access recorders and aircraft condition-monitoring systems.

Multiple data streams expand cybervulnerability

Eurocontrol contracts with Thales for cybersecurity

Big data assists routing decisions for conflict zones

Connected aircraft communicate with airline operational centers through the Aircraft Communications Addressing and Reporting System and with air traffic control facilities by controller-pilot data link communications. They use global navigation satellite systems as the positioning source for automatic dependent surveillance-broadcast signals to ground stations, which air traffic controllers use to separate aircraft.

The multiple links have "extended the attack surface to the aircraft itself," the report states, increasing its exposure to cyberattacks that can corrupt or destroy data. "These aircraft are not just connected to airline or air traffic services, but also to the wider internet, facilitated by both satellite and ground stations. The days of asserting that aircraft are 'secure' by means of isolation are over. There is now a clear requirement to secure and assure connected aircraft," it asserts.

Audit firm PwC surveyed airline CEOs in 2015 and found that 85% viewed cybersecurity as a significant risk, compared to 61% of CEOs in other industries. Pilots' electronic flight bags and inflight entertainment and connectivity systems are among systems posing cyber-risks that airlines need to manage "holistically" with aircraft manufacturers and hardware and software providers, PwC said.

Vendors are coming forward with such approaches to airline cyber-risk. Finnish company F-Secure in March announced an Aviation Cyber Security Services offering that integrates system- and component-level security assessments of avionics, data links, incident response services, training and other aspects in a single package to help airlines "secure their operations from the ground up."

Draft FAA reauthorization legislation approved by the U.S. Senate Commerce, Science and Transportation Committee last June calls for securing avionics systems. It would require the FAA "to consider revising airworthiness certification to address cybersecurity for avionics systems and to require that avionics systems used for flight guidance or aircraft control be secured against unauthorized access via passenger inflight entertainment systems."

Future aircraft could use broadband communications to transmit network data to the ground, where a security operations center would monitor the data flow for cyberintrusions in real time, much like a standard ground-based network operates, notes the Atlantic Council study. But corporate approaches to cybersecurity "tend to have higher rates of failure than critical aviation systems would support and may be otherwise ill fit for an aviation environment," it adds.

The potential drawbacks of ground-based monitoring of airborne networks could lead to a complementary need for autonomous onboard network intrusion detection. "The difficult question is whether such a model is robust enough to protect live aviation systems and if the industry wants aviation operators (pilots, air traffic controllers, etc.) to become part of the cyberincident response team," says the study.

Thales, which manufactures both avionics and air traffic management (ATM) systems, views cybersecurity in terms of risk management. "Protection is required, but cybersecurity protection is not enough," says Philippe Jasselin, lead executive for ATM cybersecurity development. "At Thales, we are working on cybersecurity resilience, recognizing that one day or another your protection will not be enough, and an attacker will succeed. Even if an attacker succeeds, you have to continue providing a minimum set of critical services for your business."

Contingency planning to preserve critical network services in the event of an outage on the ground and the use of redundant systems on aircraft are ways that aviation safety is maintained. Thales seeks to extend safety-centric contingency planning to cybersecurity. For example, sending a spoofed message over a network that impersonates a source address in order to hide the sender's identity may lead to a failure mode in a router. That would be considered low priority in terms of safety but high priority for cybersecurity, Jasselin explains.

"Cybersecurity to some extent can introduce new modes of failure which are not covered by the safety mechanism already in place today on ground and in the air," he says. "It is where we believe that new detection and new contingency procedures and techniques are required to make air transport more resilient."

On May 28, Thales signed contracts to strengthen the cyberattack detection and risk management capability of Eurocontrol, which, as Europe's "network manager," is responsible for an ATM network covering 43 countries.

One of Thales' five cybersecurity operations centers will monitor Eurocontrol's information technology (IT) infrastructure to detect threats and prevent attacks. Thales also will train personnel in cybercrisis management and replicate Eurocontrol networks and IT systems at a Cyberlab facility it opened last summer in Tubize, Belgium.

Under a separate contract, Thales and Belgian company Cegeka will develop software for Eurocontrol's Airspace Environment system.

Conflict Zones

Voluminous amounts of digital data, or "big data," can be gathered and shaped by an external provider to help airlines assess the risk of flying over conflict zones. The International Civil Aviation Organization created an online conflict-zone risk information repository in 2015 as one response to the shootdown of Malaysia Airlines Flight 17 (MH17) over Ukraine, but that has been criticized as inadequate and lacking timeliness. The European Aviation Safety Agency also publishes regular Conflict Zone Information Bulletins.

In April, Osprey Flight Solutions of Farnham, England, announced that Virgin Atlantic has signed as the newest customer of its Flight Risk Assessment System—risk analysis and management software that uses advanced data extraction, analytics and machine learning to assess flight risks. Through a "web-scraping" technique, the system collects data from 200,000 sources—including news media, social media, third-party data providers and government entities— in 60 languages, the company says. It filters out and analyzes aviation-relevant data to identify patterns and deliver instantaneous risk assessments.

Osprey sends clients rapid threat email alerts, displays trend data on system dashboards and provides custom reports. Operators can integrate the risk-assessment system with their flight-planning software and continuously monitor risk in the countries or regions along their scheduled routes, the company says.

Assessing overflight risk is one of the system's key functionalities. Osprey has divided the globe into 10 X 10-km (6 X 6-mi.) blocks; within each block, it can provide a dynamic, altitude-dependent risk assessment. That can help airlines analyze risk at any point of a flight, without being constrained by country borders or flight information region boundaries.

"We can be far more detailed about our assessments and start to open up routes that might be deemed to be unsafe," says CEO Andrew Nicholson, who started Osprey Flight Solutions in November after serving as head of aviation security with MedAire.

A warning system such as Osprey's could have helped prevent the downing of MH17, a Boeing 777-200 that was struck by a Buk (SA-11 "Gadfly") anti-aircraft missile on July 17, 2014, while flying over a contested area of eastern Ukraine. All 298 people on board were killed.

On May 25, the Dutch and Australian governments heading the incident investigation formally accused Russia of the shootdown (*AW&ST* June 4-17, p. 34). They based the declaration on findings of a Dutch-led investigative team

that traced the missile to the 53rd Anti-Aircraft Missile Brigade, a Russian Army unit based in Kursk. Russia has denied involvement and blamed the Ukrainian military.

Incidents such as the MH17 shootdown are rare; Osprey's system more often sends alerts about operational risks arising from events such as strikes, drone sightings and reports of laser pointing, Nicholson says. The company does not provide information directly to pilots, although there could be applications displayed on an electronic flight bag, he adds.

"The reason we don't do it is because of all of the operators that we've spoken to, none of them wants us speaking directly with their pilots, and for very good reasons," Nicholson says. "They need to be able to understand the situation and keep their own operational overview of the situation rather than [make] an instant decision on information that they have no control over."

Other approaches to aircraft security call for protecting access to the flight deck, arming pilots and using blast-resistant cargo containers. Each has limitations, the Congressional Research Service (CRS) found in a January report focused on the security of air cargo shipments.

The Aviation and Transportation Security Act that Congress enacted following the September 11, 2001, terrorist attacks required commercial airlines to install hardened cockpit doors, but the FAA later exempted all-cargo aircraft because of limited federal funding. "While some cargo aircraft have hardened cockpit doors to thwart potential stowaway hijackers, many do not," the CRS states.

United Airlines voluntarily installed secondary barriers on some of its passenger aircraft in 2004; they have now been phased out of the fleet. "Other airlines have not installed the barriers, and currently no U.S. air carrier aircraft have them," the CRS said.

The Air Line Pilots Association (ALPA), which represents pilots at U.S. and Canadian airlines, has called on Congress to require secondary barriers in FAA reauthorization legislation to protect the flight deck when pilots need to open the hardened door. Boeing and Airbus offer secondary barriers on new aircraft, and retrofitting lightweight barriers on existing aircraft would cost $5,000 or less, ALPA contends. Other industry sources place the cost at $5,000-12,000, the Senate Transportation Committee says.

The House version of FAA reauthorization legislation, which the chamber approved on April 27, calls on the FAA to require installation of a secondary cockpit barrier on each new passenger airliner. Draft Senate legislation also would require secondary cockpit barriers.

Reportedly, thousands of U.S. airline pilots have received training to carry and use firearms under the Federal Flight Deck Officer (FFDO) program, which was launched by the Homeland Security Act of 2002 and later extended to include all-cargo airlines. ALPA and the Coalition of Airline Pilots Associations say FFDO funding of $22 million per year has not kept pace with the program's growth and should be increased.

Use of blast-resistant cargo containers to protect against explosives "never gained traction for a variety of reasons including cost, weight and susceptibility to damage," the CRS found. "The hardened containers were primarily designed for long-haul widebody aircraft and are not universally compatible with the various narrowbody aircraft that dominate the commercial passenger airline fleet," it said.

Source URL: http://aviationweek.com/connected-aerospace/securing-aircraft-becoming-more-complex