CRS Insights

Protecting Civil Aviation from Cyberattacks

Bart Elias, Specialist in Aviation Policy (belias@crs.loc.gov, 7-7771)

June 18, 2015 (IN10296)

Cybersecurity is a growing concern for civil aviation, although the significance of reports in May that a computer security researcher hacked into aircraft control systems while flying as a passenger aboard commercial jets is still unclear. The probe into the alleged hacking incidents unfolded just weeks after the Federal Bureau of Investigation (FBI) and the Transportation Security Administration (TSA) alerted airlines to be on the lookout for passengers trying to tap into aircraft electronics and for evidence of tampering or network intrusions.

It is not just systems aboard aircraft that are potentially vulnerable. The ongoing transformation from stand-alone navigation equipment, radar tracking, and analog two-way radios to highly integrated and interdependent computers and digital networks, both onboard aircraft and in air traffic control facilities, creates inherent security vulnerabilities. In April 2015, a Government Accountability Office (GAO) study found that the Federal Aviation Administration (FAA) faces ongoing challenges to protect air traffic systems from cyberattacks, and warned that the increasing interconnectedness of aircraft systems makes them vulnerable to unauthorized remote access.

Air traffic control systems and airport and airline information technology systems have been identified as critical transportation infrastructure covered under national policy to strengthen security and resilience to cyberthreats. Although federal laws, criminal statutes, regulations, and oversight all play roles in cybersecurity, much of the responsibility rests with industry working groups that develop standards and guidelines for air carriers and equipment manufacturers to follow.

Various reports have suggested that, despite ongoing efforts to develop secure systems, many vulnerabilities remain. In 2009, a Department of Transportation Inspector General (IG) report found that FAA's increased use of web applications linked to FAA systems exposed the air traffic system to access control vulnerabilities, and identified weaknesses in FAA's intrusion-detection capabilities. In 2014, the IG found undisclosed weaknesses in FAA's traffic flow management system, a critical system interconnecting air traffic control facilities. Similarly, in 2012, the IG found that FAA had not adequately implemented security requirements for the en route automation modernization system, which supports FAA's air traffic control modernization initiative, known as NextGen.

Potential NextGen Vulnerabilities

NextGen will rely on satellite-based aircraft navigation and tracking and digital voice and data communications between controllers and pilots, tied together using an integrated information management network called SWIM. This high degree of interconnectivity and access by both FAA employees and airspace users is expected to increase the capacity of the air traffic control system and improve safety, but it raises significant cybersecurity concerns.

The backbone of NextGen is a technology called Automated Dependent Surveillance-Broadcast, or ADS-B, which is slated to replace radar as the primary means of tracking and monitoring aircraft. Some experts claim that ADS-B is inherently vulnerable to hacking, jamming, signal flooding, and spoofing because of its open architecture and unencrypted signals, and because equipment is easy to obtain. FAA disagrees with this assessment, and claims to have measures in place to insure data integrity.

GAO cautioned that FAA's current approach to cybersecurity does not adequately address the interdependencies between aircraft and air traffic systems, and consequently may hinder efforts to develop a comprehensive and coordinated strategy. While it identified no easy fix, GAO recommended that FAA develop a comprehensive cybersecurity threat model, better clarify cybersecurity roles and responsibilities, improve management security controls and contractor oversight, and fully incorporate National Institute of Standards and Technology (NIST)

information security guidance throughout the system life cycle.

Reliance on Software Assurance

For systems onboard aircraft, FAA requires security and integrity to be addressed in the airworthiness certification process. FAA notes that aviation-specific guidance set forth in various industry guidelines developed by RTCA, Inc., provides an acceptable approach, but not the only path, to FAA software certification. FAA acknowledges that the available guidance does not fully address all areas of software development and life-cycle processes, and may sometimes be misinterpreted. FAA therefore often relies on project-specific issue papers to clarify compliance requirements for various applications.

A key strategy in protecting aviation from cyberattacks has been the development and use of software assurance methods, techniques to minimize the likelihood and impact of coding errors and omissions that may cause unintended faults or expose systems to hackers. Large commercial aircraft and aviation systems manufacturers now typically collaborate with software security companies to attain high levels of assurance for software embedded in avionics equipment, but these approaches are still evolving.

Is a Comprehensive Federal Strategy for Aviation Cybersecurity Needed?

Currently, there is no single comprehensive approach to cybersecurity in civil aviation. Some private groups have recently tried to develop one. The American Institute of Aeronautics and Astronautics (AIAA) has published a general framework for aviation cybersecurity, and the International Air Transport Association (IATA) has developed an aviation cybersecurity toolkit to help airlines and other aviation organizations manage risks using a common set of tools. However, FAA has not endorsed these approaches or developed its own strategy to steer approaches to cybersecurity across the aviation system.

Congress may examine aviation cybersecurity issues more closely in the coming months as it considers FAA reauthorization. One policy question is whether ongoing efforts are adequate or whether a more comprehensive framework should be mandated. Congress may also examine options to more fully define FAA's roles and responsibilities in developing and implementing cybersecurity policies and strategies for the aviation domain. A key question for Congress is whether FAA should develop a comprehensive system-wide policy encompassing systems certification, life-cycle product support requirements, and operational regulations to address the complex cybersecurity needs that will arise under NextGen.