7-2016

# Aviation and Cybersecurity: Opportunities for Applied Research

Jon Haass
*Embry-Riddle Aeronautical University*, haassj@erau.edu

Radhakrishna Sampigethaya
*Embry-Riddle Aeronautical University*, sampiger@erau.edu

Vincent Capezzuto
*Aireon Corporation - McLean, VA*


PHOTO: TASAYU TASNAPHUN, FLICKR

# Aviation and Cybersecurity

## *Opportunities for Applied Research*

JON C. HAASS, KRISHNA SAMPIGETHAYA, AND VINCENT CAPEZZUTO

*Haass is Associate Professor, and Sampigethaya is Assistant Professor, Cyber-intelligence and Security, Embry-Riddle Aeronautical University, Prescott, Arizona. Capezzuto is Chief Technology Officer and Vice President of Engineering, Aireon Corporation, McLean, Virginia.*

(*Above*:) Technology is involved in almost every step of air travel, from check-in to baggage claim.

Aviation connects the global community and is moving more people and payloads faster than ever. The next decade will experience an increase in manned and unmanned aircraft and systems with new features and unprecedented applications. Cybertechnologies—including software, computer networks, and information technology—are critical and fundamental to these advances in meeting the needs of the aviation ecosystem of aircraft, pilots, personnel, passengers, stakeholders, and society.

Air travelers already are using aviation cybertechnologies when booking tickets, checking in at the airline counter, going through airport security, and connecting to aircraft cabin Wi-Fi and in-flight entertainment. Many of the advances, however, are "under the hood"—in the infrastructure of avionics, air traffic control, airlines, and airports—on the ground, airborne, and in space. Cybertechnologies are embedded in the time-critical fabric that controls and assures aviation operations, safety, and performance.

Despite the great gains achieved and anticipated, cybertechnologies expose aviation to a dangerous and costly world of threats. Aviation is no stranger to threats and has matured to operate amid physical adversities from nature and mankind. But one century of flight is not sufficient to master completely the art of managing the risks threatening safety and performance.

Threats to cybersecurity pose a major challenge—the unpredictability of an attack makes the risks difficult to understand. In addition, the opportunities for attacks continually grow as new services and systems are developed.

## Emerging Cyberrisks

In 1997, the aviation sector experienced one of the earliest cyberattacks, when a teenager in Worcester, Massachusetts, exploited a vulnerability in a local airport's telecommunications service infrastructure. This denial-of-service attack exposed a weakness in the system—the reliance on an infrastructure's unfailing availability.

Recent remote hacking incidents targeting airlines, airports, and air traffic control systems show that cyberrisks will only grow; airport passport control, crews, airline passengers, and baggage control systems are frequent targets.

In 2013, more than 75 U.S. airports reported phishing—e-mails that attempt to defraud users into revealing financial information. The same year, Miami International Airport experienced more than 20,000 hack attempts per day, and Los Angeles World airports blocked almost 60,000 cases of Internet misuse and 2.9 million hacking attempts.

In addition, in 2014, a Tunisian hacker team targeted U.S. airport computer and communications systems. In the summer of 2015, LOT Polish Airlines was forced to ground flights at Warsaw airport after hackers disabled the flight plans for outbound aircraft.

Cyberadvances that have assisted in aviation operations include commercial technologies, such as Wi-Fi, GPS, Internet protocols, open-source operating systems, virtualization, and cloud computing. These have made aviation systems cheaper, faster, and interoperable worldwide. But these technologies also have inherent vulnerabilities that can be targeted remotely by cyberadversaries.

Open-source, cheap, and powerful tools that can exploit vulnerabilities make external cyberattacks on aviation assets far less complicated. For example, a White Sands Missile Range test exercise demonstrated that the GPS signals used for navigating an unmanned aircraft, or drone, can be accessed remotely to divert the flight onto erroneous paths.

Simulation studies at hacker conferences have reiterated the feasibility of attacking air traffic control systems with inexpensive equipment. A cyberattack could show bogus aircraft on the screens of air traffic controllers and pilots, influencing unsafe actions and unwarranted performance losses. Moreover, the recent Germanwings flight allegedly crashed by a suicidal pilot suggests the potential for insider threats and the need for improvements in managing the people entrusted with legitimate access to the system.

Visibility and scale make the aviation industry an attractive target for malicious actions. A single, seemingly isolated, disruption of aviation—caused, for example, by a single computer failure, a weather-affected sector, or a natural disaster near an airport—can cascade quickly across the system and affect the economies of a nation and of continents for days to months. Millions of passengers can be stranded and inconvenienced worldwide, an enormous financial loss. Addressing aviation cybersecurity aggressively is critical.

## Aviation Cybersecurity

Although the aviation industry is not alone in fighting cybersecurity threats, the challenges to transportation systems—and specifically to aviation—are unique. The aviation industry is working to understand cybersecurity threats, risks, and management.

For example, the Aviation Information Sharing and Analysis Center[1] (ISAC) and the second edition of the *Cyber Security Toolkit*[2] from the International Aviation Transport Association provide guidance for airlines and strategic partners about evolving regulations, new attack vectors, and more.

Other efforts include the Cybersecurity Special Task Force of the International Civil Aviation Organization and the proposed FAA CyberAIR Act, intended to bridge the gaps in aviation cybersecurity. The goals include identifying cybersecurity vulner-

[1] a-isac.com.

[2] iata.org/publications/.


Photo: Teragorge, Wikimedia Commons

An early cyberattack on the aviation sector occurred at Worcester Regional Airport in 1997, when a teenager exploited vulnerability in the telecommunications service infrastructure.

PHOTO: KONFLIKTY.PL, WIKIMEDIA COMMONS

A LOT Polish Airlines Boeing 767. In 2015, hackers disabled flight plans for outbound LOT aircraft.

abilities, assessing threats, and finding standard mitigations to manage the risks to the system.

## Systems and Adversaries

### *System at Risk*

The aviation ecosystem is a complex system of systems—a large number of aircraft and their users are connected to a global infrastructure composed of many systems of competing airlines, national air traffic control systems, competing airport systems, aircraft stakeholder businesses, personnel, and passengers. The ecosystem also includes the natural environment within which aircraft operate.

Safety, efficiency, capacity, security, and environmental sustainability are key performance goals of this system. Cyberthreats can degrade these performance goals by compromising a combination of information, network, Internet, and other elements of the critical information infrastructure.

### *Who Is the Adversary?*

An adversary can be classified according to motivation, resources, target, attack vectors, and other characteristics. Adversaries by motivation and resources commonly include amateurs, hacktivists, criminals, insiders, spies, and terrorists.

An adversary may directly target any system asset, including ground-based systems, aircraft, or satellites, via vulnerabilities in network connectivity, software, hardware, and human-in-the-loop processes. The adversary also can compromise the integrity, authenticity, confidentiality, and availability of data. Furthermore, an adversary may target a single component—part of the air traffic control system; a performance goal of the aviation ecosystem, such as on-time flights or safety metrics; stakeholder businesses; or passengers.

In general, cyberattacks fall into three categories:

- Passive—the adversary simply listens and observes;
- Active—the adversary transmits signals or data and receives responses; and
- A passive–active combination.

Passive listening can reveal sensitive information or lay the groundwork for more active attacks. The active transmission of incorrect data, however, can prompt erroneous and inappropriate reactions from the targeted system or systems and therefore can pose the greatest threat.

## Embedding Cybersecurity

The risks, the adversaries, and the pathways for attacks are similar for a single corporate company or for a large government agency. Attacks cause losses within minutes and hours, but the discovery and response can take days.

Best practices have evolved to reduce this time gap, but even with best practices, large institutions can be breached. The adversary is global, persistent, sufficiently funded and always learning. Defeating the adversary may be difficult, but focusing on management and approaches that can hinder an attacker long enough for a response could be feasible.

Cybersecurity is not yet as embedded as reliability into the design life cycle of aviation systems. Typical aviation system concerns—such as safety, flight performance, environmental impact, fuel efficiency, and airspace security—are alien to the world of

IMAGE: FAA

FAA began using the Automatic Dependent Surveillance–Broadcast system for air traffic control in 2009.

cybersecurity. In designing a system to protect aircraft data, do programmers consider how a pilot or an aircraft mechanic would use the system? Is a cybersecure system able to perform in an aircraft emergency?

Similarly, the concepts of cybersecurity may be alien to aviation professionals. Pilots today often carry an electronic tablet containing their flight kit into the cockpit. What security precautions are appropriate for connecting the tablet to the avionics system?

The trade-offs are complex when considering ease of use, safety, performance, cost, and on-time departures with last-minute crew changes. Adding cybersecurity concerns to the design, deployment, and upgrading of modern aviation systems will increase the cost and complexity of slow processes already heavily regulated. Cyberadversaries are not encumbered by these same rules and timescales.

PHOTO: FAA

A technician rewires and installs telecommunications equipment at the Chicago En Route Center in Aurora, Illinois. The scale of interconnected technology in aviation makes the industry a target for hackers.

## Combatting Cyberrisks

Combating aviation cyberrisk requires segregating the intended function of each system and analyzing the criticality of a threat to each component. For example, communicating air traffic control data to a controller separating in-flight aircraft is an intended function distinct from the collection of passenger manifests and credit card information for ticket payments. But if all these data are uploaded to a cloud platform, an attack on that data could create a time-sensitive and life-threatening situation.

Proactively addressing security threats to the most safety-critical systems requires the expertise of the user community—air traffic controllers, maintenance technicians, pilots, and security experts—to identify and rate the potential risks and to focus the mitigation options on the most critical issues. In building systems that address security concerns, the design must allow for security upgrades as part of the natural life cycle; this requires a continuous review of threats and a secure funding stream to implement mitigating strategies.

In the aviation environment, many resilient elements within systems decrease the likelihood of an event. For example, a remote takeover of an air transport aircraft would require intimate knowledge of the systems and the ability to defeat checks built into the onboard avionics. Nevertheless, radio frequency (RF) links into the aircraft may provide a possible point of entry for the introduction of malware attacks. Many of these links—but not all—are considered strong and robust and may limit the opportunity to jam or spoof the signals without detection.

Weak RF links in the system include the Global Navigation Satellite System signal that provides critical navigation information to the pilot and transmits data to air traffic controllers via an onboard Automatic Dependent Surveillance–Broadcast (ADS-B). An independent validation process has been designed to address some of the threats to these data—secondary means are needed to validate the aircraft's location.

This secondary validation gives the pilot or controller the opportunity to confirm the integrity of the aircraft's position, inserting a pause into the decision process and arming the operator with knowledge about a possible exploit. Although this helps to mitigate the data security risk, the stress increases with the involvement of weather or other factors—the crew must decide which system to trust if the systems do not agree. Not all pathways to mitigation are ideal.

RF links are only one of many systems that require continued investigation of all the cybersecurity implications. Security must be designed into the system as part of the ongoing life cycle, allowing for

appropriate responses to known risks and for the flexibility to detect and prevent "unknown unknowns" from crippling the aviation system.

## Standards and Best Practices

The Federal Aviation Administration (FAA) recently issued a call for proposals on aircraft systems information security and protection measures.[3] The call responded to a 2015 breach and a Government Accountability Office report[4] pointing to cybersecurity concerns for increasingly electronically enabled planes and airports—both indications of the need for better cybersecurity standards and practices in the industry.

A comprehensive framework for preventing cybersecurity threats is in development, based on the National Institute of Standards and Technology's best practices for FAA's next-generation aviation system, NextGen. In addition to these steps, significant new work and research are needed to design, test, and deploy more cybersecure systems. In the United States, the Radio Technical Commission for Aeronautics has published a document, *Airworthiness Security Methods and Considerations*,[5] offering guidance on information security for continued airworthiness; these concepts will have an impact on the NextGen systems.

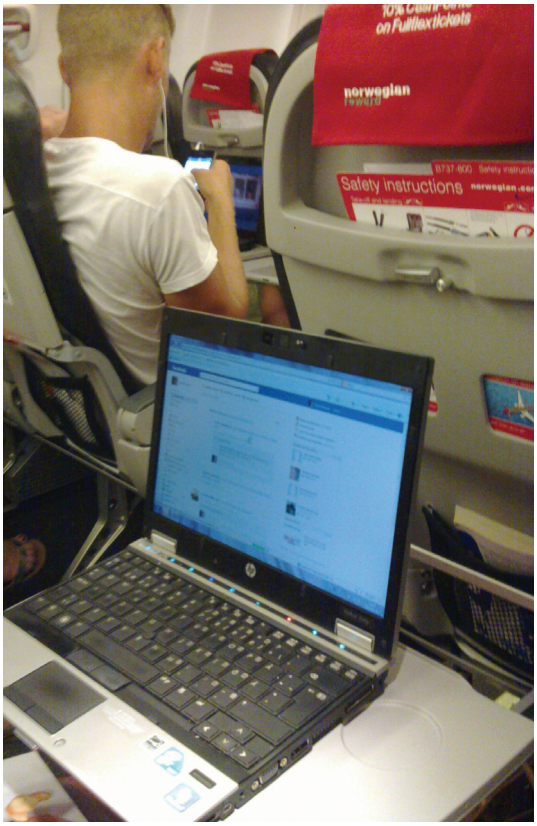
The Aviation Information Sharing and Analysis Center serves as a clearinghouse for best practices from industry and academia in addressing individual systems, as well as the encompassing environment. Airlines are racing to provide services to passengers, flight support for crew, and more efficient tools for diagnostics and maintenance. The cybersecurity of these initiatives may not be keeping pace with the rush to the competitive marketplace.

The new cybersecurity systems being deployed not only must address current threats but must anticipate the need to address current and possible future threats that were not part of earlier designs. The aviation systems in development for flight control, position, and automatic pilot capabilities must include integrity checks, authentication mechanisms, and privacy-preserving capabilities. Any communication system in the aviation industry must be considered for its potential to be blocked, spoofed, intercepted, and possibly altered in a way that may look correct but is dangerously wrong.

The best practices to identify, protect, monitor, mitigate, and update should become the framework for each stage of new system designs and upgrades.

[3] DTFACT-16-R-00037.
[4] GAO-15-370.
[5] DO-356.

PHOTO: KONSTANTINOS KOUKOPOULOS




In-flight Wi-Fi and other passenger services also are vulnerable to cyberattack.

## Research and Development

FAA's recent call for proposals on cybersecurity measures is a step in the right direction for investigating and recommending solutions to some of the known weak links in proposed communication systems. These include research into the impact of larger volumes of UAS traffic and increased reliance on computer-to-computer signaling for decisions from aircraft spacing to weather avoidance.

Other areas for investigation include privacy issues involving access to the precise positioning and identification of air traffic in real time. Satellite-based systems can be exploited for communication channels, and positioning system signals can be delayed, altered, or blocked.

Vulnerabilities are not in the avionics systems only. Crews, their authentication, security practices for devices, route planning, and integration in the cockpit present areas to address. The insider threat, described in more detail in the article on page 44, can never be solved via technology alone.

Airports and airlines are an increasingly complex system of industrial control systems, from lighting to baggage handling to maintenance, in addition to passenger manifests, cargo information, and flight planning. As society increasingly relies on electronic devices, the security of the Airport of Things is ripe for definition and understanding.