Avionics Security Assessment

Assessing the avionics system to defend against potential large-scale cyberattacks

The aviation network carries over 2.6 billion passengers a year. It employs about 8.6 million people in the US alone. And, its impact on the global economy is estimated at $2.2 trillion.[1] So while the aviation industry faces many of the same security threats as corporate enterprises, the risks can be infinitely greater. With the evolution of security technology, more and more aviation systems are based on commercial off-the-shelf products and solutions with an increased reliance on the operating systems such as Linux, Windows, and on protocols such as IPV6. The result of moving forward is moving backwards as the widespread adoption of these technologies has unleashed increased vulnerabilities and greater risk to the avionics systems.

Benefits

- Feel confident that your avionics systems are secure through expert vulnerability testing and investigation.
- Be assured that our risk-based approach will help you prioritize your security investments, focusing on the most critical threats first.
- Show due diligence and proof of attestation to your customers indicating that your systems have undergone comprehensive scrutiny from the industry experts.
- Employ a proactive approach to security defense and protection.
- Know that our team will analyze your risk and the potential impact to your airline—incorporating that into our risk calculations.
- Gain knowledge of testing techniques, issues, and remediation for future strategic planning or issues.

Your Challenge

As avionics software becomes more sophisticated to keep up with other technological dependencies, the opportunity for error also increases. The challenges you face include the growing need to integrate safety and security measures into your software while carefully managing systems in an effort to counter cybercriminal activity. At the core of these challenges is the architecture of the aviation industry and its dependence on Information and Communications Technology (ICT) to operate the global air transport system. The ICT includes distributed networks, and interdependent physical and cyberspace functions, as well as governance constructs that involve multilevel authorities, responsibilities, and regulations.

According to the AIAA, the global aviation system is one of the most complex and integrated systems of ICT in the world, which makes the system a potential target for a large-scale cyberattack. Therein lies your challenge.

Our Value

Foundstone® Services—part of the Intel® Security product and services offering—balances the strategic benefits of business consulting with a tactical, hands-on approach to technology consulting and security training. Our avionics methodology is designed to give you peace of mind that your cyber network is analyzed and fortified to reduce risk. Our consultants have skills in both application and network security, which are required when performing complex security assessments. The Foundstone aircraft assessment methodology is based on our experience performing security assessments on the Boeing 777 for a major airline company.

intel Security

Related Foundstone Services

- Web Application Assessment.
- Web Services Security Assessment.
- Thick Client Assessment.
- Mobile Application Assessment.
- Security Code Review Assessment.
- Application Threat Modeling.
- Software Security Maturity Assurance (SSMA) Assessment/ S-SDLC Gap Analysis.
- Writing Secure Code Training (Java, .Net, C/C++).
- Secure Coding Policies and Standards.

"When I was asked why I chose Foundstone Services, I thought, 'would I want to hire a company that runs the tools and reads the books, or should I hire the company that writes the tools and writes the books?' The choice was simple."

—Foundstone client

The Avionics Assessment Methodology

Our approach to performing avionics assessments starts with threat modeling of the aircrafts and the related systems as recommended by the AIAA report, "A Framework for Aviation Cybersecurity." During our on-site threat modeling engagement, Foundstone consultants meet with key stakeholders including avionics engineering personnel, and focus on these key opportunities:

- Radio interfaces that can deliver data, specifically those that affect navigation and flight safety such as the Satcom, Traffic Collison Avoidance System, Instrument Landing System, Global Positioning System, and Distance Measuring equipment.
- Cabin and AIMS systems' data cross-over paths.
- Cabin and electronics bay potential ingress and egress points.
- Data loaders (software parts, FOQA—Flight Operational Quality Assurance).
- In-flight entertainment systems and in-flight Wi-Fi service.

Both internal and external threats are reviewed during this engagement—with emphasis on threat actors like the aircraft crew, air traffic controllers, aircraft ground technicians, pilots, catering crew, cabin crew, cleaning crew, passengers, operations control center, and remote attackers. After this review, our consultants test all the viable internal and external threats identified during the threat modeling engagement.

Final Report and Summary

As our consultants complete their investigation and testing, the results and recommendations are captured and communicated throughout the engagement. Our team delivers a comprehensive technical report in the format of your choice. After thorough review-board approval, we deliver the report broken into the following categories:

- Executive Summary.
- Summary of Strengths.
- Benchmark Data upon request.
- Testing Notes.
- Report Card.
- Strategic Recommendations: People, Process, and Technical.
- Findings and Recommendations.

Why Foundstone Services

Enterprises should never feel like they are on their own when it comes to protecting critical corporate digital assets—especially in an emergency. Foundstone Services is your first responder, available to help you quickly identify a breach and remediate further damage.

We are seasoned security consulting experts skilled at identifying network and application vulnerabilities, providing remediation recommendations, and helping organizations design iron-clad security programs and enforceable policies. Couple this prevention with security training from our industry-leading experts, and your organization will be well-prepared to combat emerging online threats and defend your valuable assets.

Learn More about Foundstone Services

Fill the gaps in your information security program with trusted advice from Foundstone Services—part of the Intel Security global professional services organization that provides security consulting, customized product deployments, and training and advisory services. Let our consultants help your organization assess current policies, create new programs that meet compliance goals, and cost-effectively prepare for security emergencies. Speak with your technology advisor about integrating our services. You can get more information at **www.foundstone.com**.

1."A Framework for Aviation Cybersecurity," An AIAA Decision Paper, August 2013

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com