Avionics Cybersecurity Research Test Bed

Research tool to develop aviation focused cybersecurity defenses

Aviation is critical to the rapid and safe transportation of people and goods on a global scale. Protecting aircraft from cyber-based threats is paramount to national security and maintaining confidence in air travel and transport.

To enhance the safety of aviation components from the threat of cyberattacks, Idaho National Laboratory (INL) has partnered with the Department of Homeland Security and the Aviation Cyber Initiative (ACI) to build the Avionics Cybersecurity Research Test Bed (ACRT). The ACRT provides the infrastructure and tools necessary to research emerging threats to aircraft avionics that result from specification, implementation, and operational based vulnerabilities.

TAXI AND TAKEOFF

The interdependency of avionics systems, reliance on common technologies, and growing realization of advanced cyber threats highlight the need for an effective means to evaluate avionics systems cybersecurity. The ACRT provides a resource where government and industry partners can investigate avionics system cybersecurity, experiment with technology and standards in a controlled environment, perform exploratory system vulnerability research, promote development of mitigation strategies, and inform the community on cybersecurity principles. INL is responsible for the design, implementation, and management of the ACRT.

CLIMB AND MAINTAIN

The ACRT enables research to identify vulnerabilities and develop/evaluate mitigation strategies. Vulnerabilities in avionics systems fall into three main categories:

Specification Vulnerabilities: Specification vulnerabilities result from inherent weaknesses in design specifications, standards, or protocols. For example, communications standards that do not support encryption. Avionics components must comply with multiple standards that cover form and fit, interfaces, wired, and wireless communications. Exploration of potential vulnerabilities inherent to these standards is critical to ensuring aircraft and avionics components can safely communicate.

Implementation Vulnerabilities: Implementation vulnerabilities result from flaws in software and firmware source code. Flaws, such as buffer overflows, fall into this category. The ACRT

Idaho National Laboratory

The Avionics Cybersecurity Research Test Bed (ACRT) is uniquely suited to address major challenges in aviation focused cybersecurity assessments:

- Perform controlled cybersecurity research and analysis.
- Initiate over-the-air fuzzing of aircraft communication and data links.
- Execute aviation data bus fuzzing and data bus standards assessments.
- Assess avionics software loading formats and standards.
- Perform device-level evaluations.
- Train personnel to perform assessments against avionics systems.
- Conduct acceptance evaluation of system deployments and software upgrades.
- Examine effects of cyber exploits in a system-of-systems environment.

allows researchers to discover implementation vulnerabilities before bad actors do.

Operation Vulnerabilities: Operational vulnerabilities are the result of flaws introduced through insecure configurations or insecure procedures. These vulnerabilities may be installation or owner dependent and can be reduced through the use of best practices. The ACRT allows researchers to determine best practices and secure configurations that will reduce the risk associated with operational vulnerabilities.

IN-FLIGHT SERVICE

The ACRT provides capabilities targeted toward aviation systems via a flexible test environment that enables communications between major avionics components. The ACRT also provides the ability to perform over-the-air fuzzing and protocol assessments of common aviation standards. The ACRT provides the tools to perform cybersecurity assessment tasks in the unique aviation environment to include traffic injection and spoofing, fuzzing, message reverse engineering, pivoting, and proof-of-concept demonstration.

UNIQUE CAPABILITIES:

- **Modular and Expandable:** The ACRT can be configured or modified to integrate a variety of avionics components. The ACRT can transmit to 12 distinct devices and receive from 48 distinct devices using standard aviation bus communication standards.
- **Real-World Data Link Traffic Repository:** ACRT users have access to real-world data link traffic captured from over 8,000 distinct aircraft. The data link traffic library provides users with the data needed to develop test cases based on realistic scenarios across a variety of airframes.
- **Generate Custom Traffic:** The ACRT supports bit level control of both data-bus and radio frequency formats common to aviation. Users have unlimited flexibility to precisely control communications with target devices. This level of control enables tests such as fuzzing, edge case, race conditions, etc.
- **Monitoring Taps/ Instrumentation:** The ACRT provides both hardware and software-based data taps to intercept, capture, and inject traffic for analysis. Users can monitor and instrument devices using the vendor provided software interface or with their own bus or radio frequency capture devices, leading to controlled and repeatable test cases.

These features combine to give ACRT users the ability to perform cybersecurity testing of avionic system throughout their lifecycle in an operationally relevant environment.

FINAL DESCENT

The ACRT provides government and industry partners a capability to perform extensive research and development and gain insight into the cybersecurity threats targeting commercial aircraft. Results will enhance aviation cybersecurity and lead to greater coordination, collaboration and information sharing across the aviation ecosystem.

FOR MORE INFORMATION

Technical contact
Ollie Gagnon
ollie.gagnon@inl.gov

General contact
Ethan Huffman
ethan.huffman@inl.gov

www.inl.gov

A U.S. Department of Energy National Laboratory

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy. INL is the nation's center for nuclear energy research and development, and also performs research in each of DOE's strategic goal areas: energy, national security, science and the environment.