Using Digital Twins as a Sandbox for the Evaluation of Cyber Attacks on Avionics Networks

TA: Hridhay Monangi
BOEING MENTORS: Josh D. Eckhardt, Dr. James L. Paunicka, Dr. Douglas A. Stuart

PROJECT SUMMARY

Problem Statement
• The discussion of cyber attack vectors specific to avionics networks is limited within academia.
• The synergy of computer science and civil aviation technology allows for the development of new approaches to cyber security problems in aviation.

Research Goal
• Previous year’s research consisted of using a digital twin based off document ARINC 811 which outlined subsystems of the network.
• Research was presented at AIAA SciTech Conference (Kuleshov, et al. 2024)
• This year’s goal was to simulate a new attack vector and improve fidelity of the model.
• To simulate an attack that involves the Automatic Dependent Surveillance-Broadcast (ADS-B).
• To improve the fidelity of the model we included a replica of the 1553 standard military-based data bus (MIL-STD-1553).

METHODOLOGY: ATTACK VECTORS AND DEFENSE

ADS-B Attack Vector
• An attacker sends spoofed ADS-B messages into the airspace.
• The spoofed plane is on collision course with the real plane, received on these messages.
• The distance of the attacker from the plane is calculated using the received signal strength.
• This calculated distance is compared to the claimed location from the ADS-B message.
• Divergent values indicate a spoofed message.

Military Standard 1553 Data Buses
• A Python-based processes is used to capture network and system configurations of real aircraft.
• The Python library we wrote imitates MIL-STD-1553 data bus protocols.
• Bus controllers facilitate communication between all terminals on the network.
• Currently, there is no protection against a remote terminal acting as a bus controller, allowing a malicious system to arbitrarily overwrite data on another system.

ACARS Attack Vector
• A rogue signal is sent to the aircraft with a fake message holding improper data requested.
• Due to the lack of verifiability, message is displayed, and unverifiable data is shared.

Passenger Manifest Attack Vector
• Threat Actor sends a fake Passenger Manifest file.
• Unauthorized access to PM can result in:
  o Attacker uploading additional information (i.e., adding names) to give boarding privileges to unauthorized passenger.
  o Attacker deleting or altering PM to cause delays to flight schedule.
• Message Authentication Code (MAC) is used to validate manifests.

ATTACK VECTOR CONTEXT

Automatic Dependent Surveillance–Broadcast (ADS-B)
• ADS-B is a surveillance technique used by aircrafts to broadcast their identity to the outside world.
• ADS-B messages display various information about the aircraft including coordinates, altitude, speed, etc.
• Pilots may control the aircraft based on the data received from ADS-B messages.
• Currently, ADS-B data is publicly available and lacks protection against spoofing attacks.

MIL-STD-1553 Data Bus RT-BC Fault
• In Military Standard 1553, data bus protocols consist of Remote Terminal (RT) systems and Bus Controllers (BC).
• Data buses are used to facilitate information exchanged between systems in an aircraft.

Aircraft Communication Addressing and Reporting System (ACARS)
• ACARS is a communication means pilots use to interact with Aircraft Traffic Control (ATC) centers, airline services, or third-party services via plaintext messages.
• Data is transmitted and received via ground stations or satellite using the High Frequency or Very High Frequency bands.
• ACARS lacks cryptographic security and verification methods, making them susceptible to spoofing.

Passenger Manifest
• A flight’s Passenger Manifest (PM) includes names, passports, dates of birth, seat numbers, etc.

REFERENCES:

The Data Mine Corporate Partners Symposium 2024