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

TEAM MEMBERS: Alisha Gadaginmath, Sanjana Gadaginmath, Yury A. Kuleshov, Kabir Nagpal, Katie B. O'Daniel, Dalbert Sun, Lucas Tan, Korel Ucpinar, Nathan L. Veatch, Naren Velnambi
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)

Figure 1: Picture of our team's trip and presentation at the AIAA SciTech Conference

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 flights Passenger Manifest (PM) includes names, passports, dates of birth, seat numbers, etc

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 based 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:
  - Attacker uploading additional information (i.e., adding names) to give boarding privileges to unauthorized passenger
  - Attacker deleting or altering PM to cause delays to flight schedule
- Message Authentication Code (MAC) is used to validate manifests

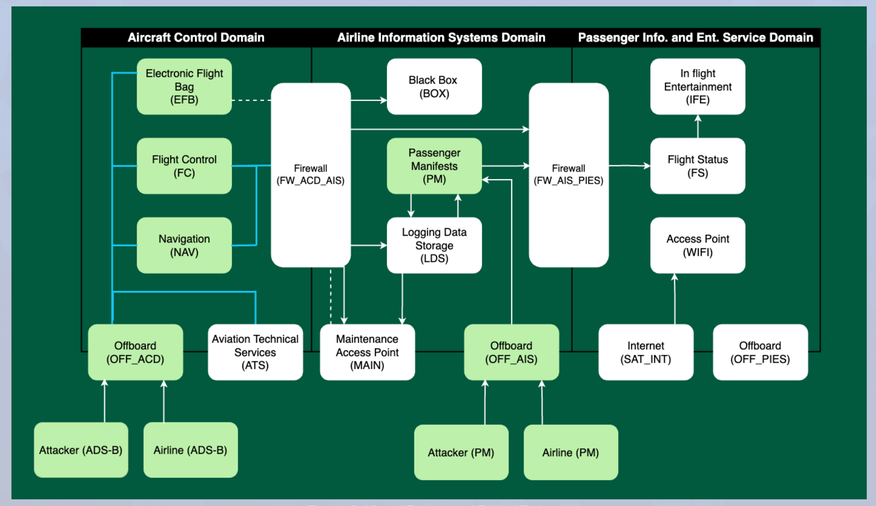

Figure 2: Visual Diagram of Digital Twin

References:
Boeing. (2022, August 26). *BOEING OVERVIEW* [PowerPoint Slides]. TDM 51100-037/110 Course, The Data Mine, Purdue University, West Lafayette, IN, USA.
Boeing. (2023). *Boeing 2022 Jet Snowflake Desktop Wallpaper (v.2)* [Poster Background]. Boeing Store. https://www.boeingstore.com/pages/wallpapers
Huffaker, J. (2022, September 14). *Cyber Security in Aviation* [Seminar]. CERIAS Security Seminar Series, Purdue University, West Lafayette, IN, USA. https://engineering.purdue.edu/AAEFlightPlanNews/news/events/cerias-security-seminar-series-presents-james-huffaker-914

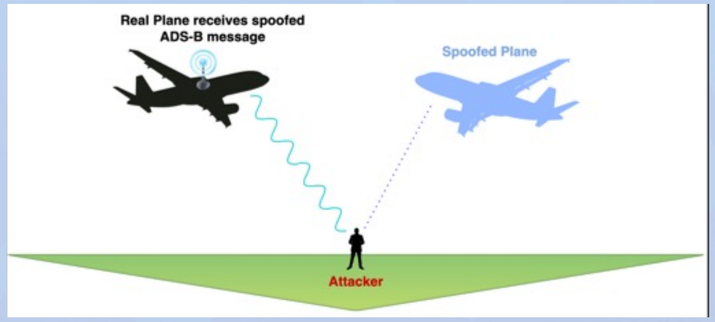

Figure 3. Visual Diagram of ADS-B attack vector

ANALYSIS OF RESULTS, DISCUSSION, AND CONCLUSIONS

Analysis of Results
- The inclusion of the new Data Bus protocols improved the fidelity of the model
- Attacks and defenses were also added and meant to be realistic but were simplified for the simulation. These contributed to the attack vectors we had sought to add as well

Discussion
- We tested many attack vectors to encourage ideas for different defenses
- The ADS-B attack vector had been an ongoing concern in the industry. Our work was a proposed solution to the concern

Conclusion
- The research allowed each student to obtain practical skills in brainstorming and approaching new challenges to cyber security in commercial aviation
- The success of this class provides additional support for the introduction of cyber security competence with specific applications, such as aviation, among a broad range of higher education students in STEM majors

CHALLENGES & LIMITATIONS

- Documents like ARINC 629, a standard used in aircraft systems, have limited availability to the public
- Assumptions and abstractions were also made to replicate MIL-STD 1553
- The plane receiving the ADS-B data follows a generated flight path for simplicity as opposed to finding a historical example of a flight data that would fit our ADSB attack scenario

FUTURE GOALS

- Continue increasing the fidelity of the existing prototype of the Digital Twin
- Researching supply chain issues in aviation cybersecurity and linking them to the model inputs and/or outputs
- Designing simulations of other attacks to take advantage of the sandbox tool potential