CERIAS

The Center for Education and Research in Information Assurance and Security

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

Alisha Gadaginmath, Sanjana Gadaginmath, Yury A. Kuleshov, Hridhay Monangi (TA), Kabir Nagpal, Katie B. O'Daniel, Dalbert Sun, Lucas Tan, Korel Ucpinar, Nathan L. Veatch, Naren Velnambi

Problem Statement

- Conventional methods of the evaluation of cyber attacks on avionics networks do not meet the requirements of the ongoing Industry 4.0 (I4.0) revolution
- Digital twins have not been widely used in avionics networks in academia

Research Goals

- To increase the fidelity of the existing prototype of the Digital Twin (Kuleshov et al., 2024)
- To design an Avionics Networks Sandbox using the Digital Twin
- To demonstrate the feasibility and value of the Avionics Networks Sandbox for the emulation and evaluation of cyber attacks and defenses

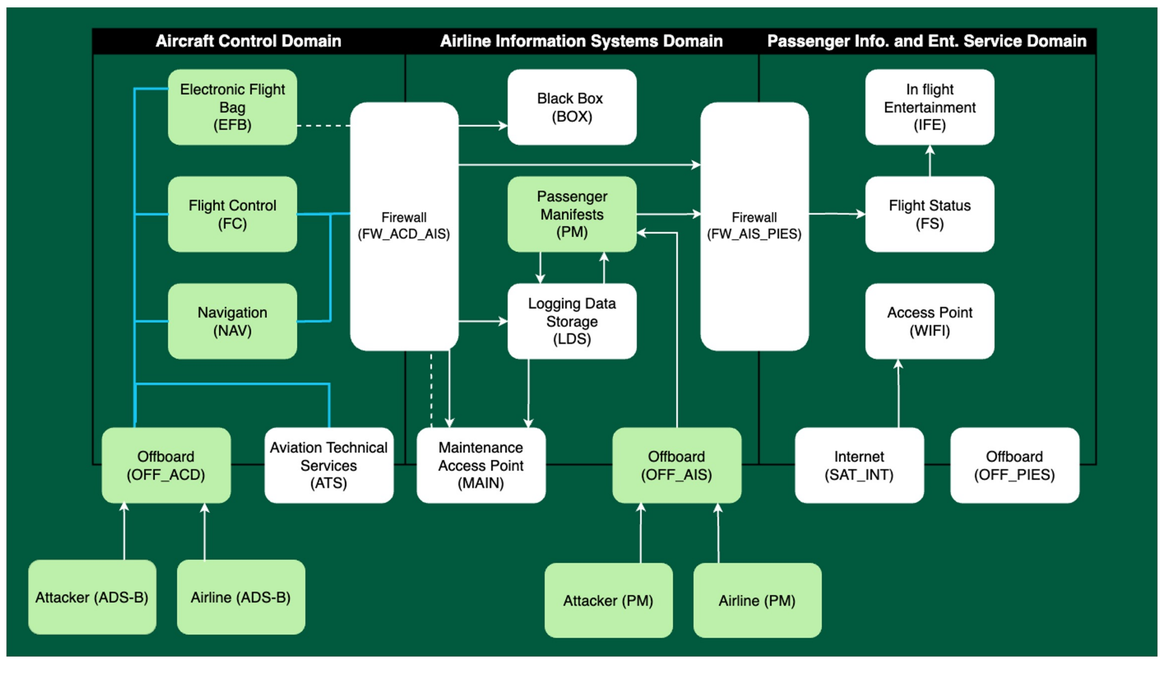
ADS-B ATTACK VECTOR

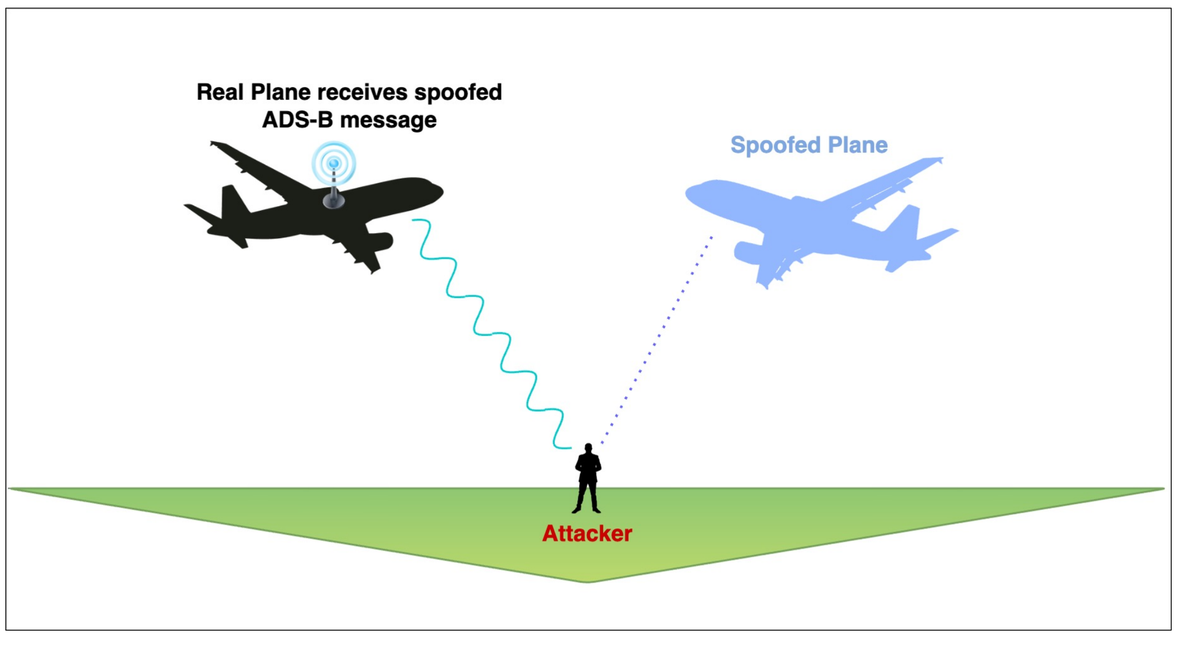
- Currently, the ADS-B lacks protection against spoofing attacks
- A fake message containing relative position data can disrupt aircraft trajectories
- Attack begins with a message being read at the Offboard ACD
- Data is sent to the Navigation system to be decoded and then to the Electronic Flight Bag to be displayed
- Pilot responds based on data displayed when it is read at the Flight Control system

ADS-B DEFENCE

- The distance to the signal origin is calculated using the RSSI
- This value is compared to the distance to the plane as inferred by GPS coordinates from the ADS-B messages
- Divergent values beyond a set threshold indicate a spoofed message

DIGITAL TWIN





IMPLEMENTATION OF MIL-STD 1553 DATA BUS

- Data bus standard in use in military aircraft avionics systems since the early 1970s
- All communication must be initiated by the bus controller
- One data bus system in the ACD: Flight Control acts as the bus controller while other systems act as remote terminals

CHALLENGES & LIMITATIONS

- Documents like ARINC 629, a standard used in aircraft systems, have limited availability to the public. Assumptions and abstractions were made to replicate MIL-STD 1553
- The digital twin uses publicly available repositories of real ADS-B messages for testing, though the repositories do not cover all cases, and do not include spoofed messages
- The plane receiving the ADS-B data follows a generated flight path rather than a publicly available one

Reference

Kuleshov, Y. A., Nagpal, K., Ucpinar, K., Gadaginmath, A., Gadaginmath, S., O'Daniel, K., Sun, D., Tan, L., Veatch, N., & Monangi, H. (2024). Cyber Attacks on Avionics Networks in Digital Twin Environment: Detection and Defense. In *AIAA SciTech 2024 Forum* (p. 0277). American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2024-0277

PURDUE UNIVERSITY

CERIAS