Matthew Preston
Georgia Institute of Technology OMSCY CS6727 Practicum Project Proposal

Lowering Avionics Bus Trust: Moving ARINC429 Bus Architecture Towards Zero Trust.

Section 1: Problem Statement

In avionics, bus architectures such as ARINC 429, MIL-STD-1553 and ARINC 629, play critical roles for aircraft computer communication. Designed in the 1960s and 70s, these systems are robust and reliable, but are no longer resilient to modern cybersecurity threats. With respect to the project of ARINC 429, the problem with these bus architectures is that they are inherently the opposite of zero-trust. If an adversary gains access to the bus, they can potentially issue unchecked commands to line replaceable units (LRUs) in cyber-physical systems, leading to catastrophic kinetic effects. This practicum aims to explore and develop solutions to enhance the security of the ARINC 429 bus architecture by engineering and enforcing zero trust security measures, thereby mitigating the risk of unauthorized access and malicious commands.

Section 2: Problem Relevance and Motivation

In 2022 The White House commanded government agencies to move towards zero trust cybersecurity principles. This policy was stated in Executive Order 14028 and explained further in White House Memorandum M-22-09. Therefore, it is safe to say that the US Government is interested in securing its technologies by applying a Zero-Trust framework to subcomponents of US Government systems. Due to the potential of a cyber-attack having kinetic effects that could cause loss of life and negatively impact multimillion dollar assets that civilian avionic groups and airplane passengers rely on, the safety and security of aircraft components is further underscored. Furthermore, other governments and organizations around the world have airplanes with the same or similar technologies.

The limited 11-week timeline and somewhat limited resources available will drive the scope of this problem. Because of its use in DoD systems and the defense industry, MIL-STD-1553 is likely of most interest to the US Government, which makes it more sensitive and prevents one from obtaining pertinent data. Therefore, this project will focus on the civilian equivalent: ARINC429. ARINC429 is mostly used in civilian aircraft such as the Boeing B737, B747, and B767, the AirBus A320, and A340, and the McDonnel-Douglas MD-11, but it is also used in military systems that derive from similar civilian aircraft. The aviation industry's reliance on legacy systems underscores the impact of this security problem.

Section 3: Deliverables and Project Plan

I expect to develop and deliver the following by the conclusion of this practicum:

1. A simulated environment with visualization and code-based interfacing tools of an ARINC429 bus. This would be an extension of current free and open-source resources for ARINC, such as pyARINC429 (https://github.com/aeroneous/PyARINC429). Current ARINC429 simulation is non-existent.
2. A simple hack/attack implemented on this simulation that can demonstrate the impact of various scenarios. It will assume compromise of the plane to ARINC429 components – as one should with a Zero Trust mindset. For example, assuming the ARINC429 transceiver component has been compromised, the hack would then be getting that component to send out valid commands with catastrophic effects, like turning the engines off or putting the plane into a downward trajectory.
3. (Building off the simulated ARINC429 bus with LRUs, would amount to building) A digital twin with a virtual monitoring solution that includes malicious commands for the simulated ARINC429. This solution would be a twin of the bus with expected behaviors coded in, allowing it to show what the bus should look like devoid of an attacker at any moment, and allowing a human to be a manual monitor of the bus.
4. A rules-based intrusion detection unit for ARINC429 data frames.
5. A machine-learning approach to have a computer learn to differentiate between normal traffic and a malicious command, and then inserting it in the bus or transceiver component to stop the generated malicious activity. This would have to be optimized to fit and run on smaller components since it is preferable to have the smallest and fastest device added to a plane, rather than large computers.
6. A comparison of the strengths of each approach to determine which specific approach, of if a mixed approach is the best solution. Each solution will be evaluated on its reliability as well as its minimal impact on system robustness, computing/resource needs, and weight.

   I have the following stretch goals:

7. Extending the simulation environment to real work components, having a small and simple physical home lab.
8. The ultimate stretch goal of this project would be to implement an ARINC429 bus on a small UAV, execute the hack from deliverable 2, and then using any of deliverables 3 through 5 to stop it. This could lead to for follow on work if more time and financial resources are provided.

References:

- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- https://github.com/aeroneous/PyARINC429
- https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- https://whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

- https://www.swri.org/podcast/ep64
- https://www.astronics.com/avionics-databus-tutorials
- https://www.aim-online.com/wp-content/uploads/2019/07/aim-tutorial-oview429-190712-u.pdf
- https://www.instructables.com/Interfacing-Electronic-Circuits-to-Arduinos/