Secure Avionics Flight Firmware Installation Routine System Design

MITRE eCTF 2022
Team **Cacti**
University at Buffalo

1 Introduction

This section presents the entities and communication channels in the system.

1.1 Entities

The following summarizes the entities in the system.

- A SAFFIRE bootloader is the main entity of the system to ensure the secure loading of flight configuration data and firmware with version updates on the device. When the SAFFIRE bootloader receives commands to boot the firmware, it is responsible for putting firmware on SRAM and handover the execution to the firmware. Moreover, the bootloader is also responsible for providing a readback feature of the firmware and configuration data to an authenticated host.
- Host is a general-purpose computer in the secure facility, which is responsible for generating protected firmware and configuration data images.
- EEPROM on the Tivaware device is a hardware component accessible to the bootloader, which can be used to store data with access permissions.
- The firmware in the avionic device contains the logic to control the flight during flight. The firmware gets the flight itinerary from the configuration files. As the flight travel is dependent on this logic and data the bootloader needs to ensure that no malicious code or data is loaded on the device.

2 Attack Models

The attackers can carry out the following attacks:

3 Our Design

3.1 Key Generation and Storage

3.2 Firmware and Configuration Data Protection

3.3 Readback Host Authentication

3.4 Prevent Version Rollback

3.5 Build Process

Describe the important changes in build process.

4 Implementation

4.1 Critical Functions and Files