Category: Engineering

cFS Cryptography Library

Intern: Aman Thanvi, Mentor: John Lucas

University of Maryland, College Park - College of Computer, Mathematical and Natural Sciences, 2300 Symons Hall, 7998 Regents Dr, College Park, MD 20742

Mission Engineering and Systems Analysis Division, Components & Hardware Systems Branch, NASA Goddard Space Flight Center, Mail Code 596, Greenbelt, MD, 20771, United States

The CCSDS Space Data Link Security Protocol is a data processing method for space missions that need to apply authentication and/or confidentiality to the contents of Transfer Frames used by Space Data Link Protocols over a space link. The cFS Cryptography Library effort aims to provide a software-only solution using the latest CCSDS Space Data Link Security Protocol – Extended Procedures (SLDS-EP) to secure communications between a spacecraft running the core Flight System (cFS) and a ground station. Leveraging a software-only solution allows missions to easily achieve compliance; projects designed without security as a focus can trade processing power utilizing this software solution to comply with the latest NASA recommendations for space mission security (NASA-STD-1006). In addition, this software-only solution leverages the standard Command Ingest (CI) and Telemetry Output (TO) cFS and Cryptography Library (CryptoLib) applications, enabling flexibility, modularity, and reuse across multiple NASA missions (i.e., NASA GSFC SmallSats).

The focus of this session's efforts was to streamline and refine the CryptoLib platform, bringing it closer to a mission-operational state ahead of its first major application with the launch of the Geostationary Transfer Orbit Satellite (GTOSat). A virtualized environment running NOS^3 and COSMOS was used throughout the development process to verify the functionality of new builds. Figure 1 represents the target functionality of CryptoLib at the beginning of this session. The aim was to refactor and streamline the Spacecraft layer and, time permitting, fully build out the Ground Station infrastructure, as seen in Figure 1. Figure 2 represents the achieved and verified the functionality of CryptoLib in this session; its initial codebase was significantly restructured to satisfy target functionality and requirements and mission-readiness guidelines while maintaining compliance with NASA-STD-1006. Most notably, the CI and TO functionalities were restructured entirely, while the Spacecraft 'Process Security' (TC_Process) and 'Apply Security' (TC_Apply) functionalities are in the process of being re-prototyped.

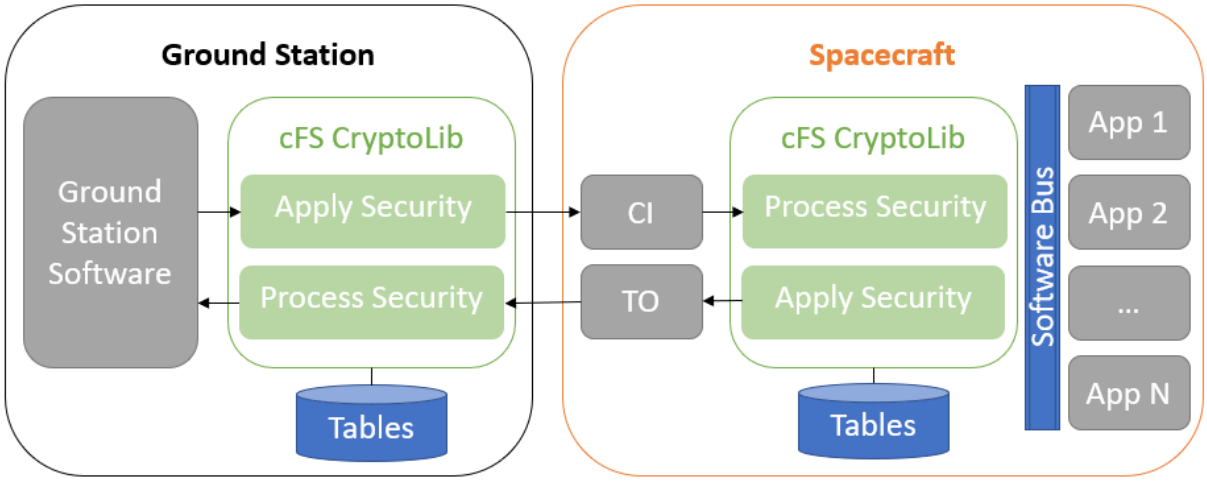

Figure 1: CryptoLib software diagram before modification to baseline functionality.

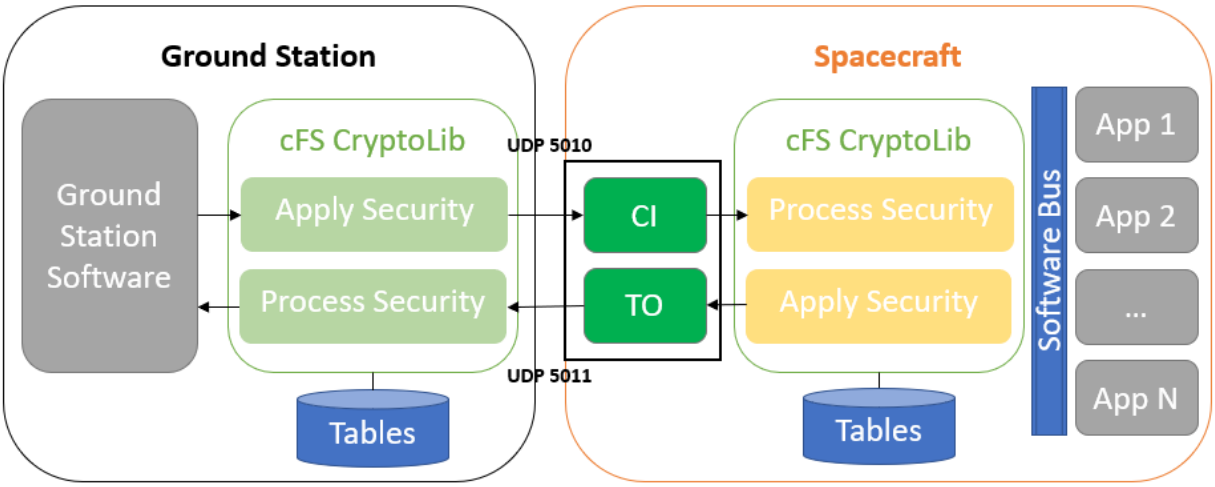

Figure 2: Refactored and verified functional CryptoLib