57th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Mickael Bonjour
Cysec SA, Switzerland, mickael.bonjour@cysec.com

Mrs. Natacha Linard
Cysec SA, Switzerland, natacha.linard@cysec.com
Dr. Louis Masson
Cysec SA, Switzerland, louis.masson@cysec.com
Mr. Laurent Thoeny
Cysec SA, Switzerland, laurent.thoeny@cysec.com
Mr. Sylvain Willy
Cysec SA, Switzerland, sylvain.willy@cysec.com

ENHANCING SPACE CYBERSECURITY:
A COMPREHENSIVE AND EXTENSIVE TESTING FRAMEWORK FOR SDLS IMPLEMENTATIONS

Abstract

Ensuring data security for satellite operations and communications has become a critical issue for the space industry. New communication standards attempt to address this issue. The Space Data Link Security (SDLS) protocol is one such standard, aiming to add security features to the CCSDS data link layer protocols, e.g. Telemetry Telecommand (TM/TC). This protocol is complemented by a suite of Extended Procedures to provide secure channel administration and over-the-air rekeying procedures. The appearance of new standards has led to the need to evaluate and verify the interoperability of their various implementations.

This paper addresses the gap in current testing methodologies of the standard by introducing a comprehensive framework designed to assess SDLS standard implementations. While institutional tests between NASA, CNES, and ESA have been conducted, the presented research endeavors to promote the space industry's perspective on SDLS and challenge its interpretation by the industry's actors. This is done by offering a framework to test the interoperability between a multitude of SDLS implementations, and in particular with respect to SDLS Extended Procedures.

The primary objective of this research is to contribute to the consolidation of the industry's understanding of the SDLS standard and to facilitate its continuous evolution. A detailed description of a test platform and its components is presented: a link proxy that can replicate man-in-the-middle attacks and other threat scenarios in data links; utilities enabling access to internal Security Associations and Key databases to check their state; and finally a dynamic instantiation of SDLS implementations. A critical aspect is the implementation of a robust test suite using the Robot framework. This allows the user to quickly add comprehensive tests using implemented keywords that don't require extensive technical knowledge except for a high-level understanding of the standard.

The presented work defines a complete test campaign encompassing various test cases, addressing ApplySecurity, ProcessSecurity test vectors, as well as Extended Procedure scenarios. Thanks to a rigorous evaluation, the framework ensures a thorough examination of the SDLS standard's security features across diverse implementation scenarios and attack scenarios.

The results of this testing campaign demonstrate a substantial added value in terms of confidence in the security features provided by the SDLS standard and its implementations. Successful tests have

been performed on various backends, including NASA Cryptolib, and CYSEC's implementation with SATLINK. These achievements not only contribute to the current understanding of SDLS security but also provide impetus for the standard's continuous improvement.