56th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Dr. Louis Masson
Cysec SA, Switzerland

Mr. Mickael Bonjour
Cysec SA, Switzerland
Mr. Sylvain Willy
Cysec SA, Switzerland
Mr. Laurent Thoeny
Cysec SA, Switzerland

DEVELOPING A CCSDS COMPLIANT PLATFORM TO SWIFTLY AND RELIABLY SECURE CURRENT AND FUTURE SPACE COMMUNICATION LINKS

Abstract

The growth of the space industry's private sector has been steadily gaining momentum through the proliferation of NewSpace companies. This increase in satellite services provides undeniable value to humankind's economic and scientific interests, albeit with added risk to the safe use of space. Large satellite constellations combined with expansive ground station and terminal networks provide a wide and vulnerable attack surface for cybersecurity threats, as demonstrated by the attack on Viasat modems on February 24$^{\text{th}}$ 2022. In addition to threatening services, these events may harm access to space as such attacks on in-orbit spacecraft pose a risk of rendering them inoperable and non-compliant.

In light of traditional approaches to spacecraft and communication systems design, security considerations and solutions in the space industry have frequently been dissociated from the design of data link protocols and are sometimes added as an afterthought. Recent standardization efforts have aimed to address this. The Consultative Committee for Space Data Systems (CCSDS) published a security standard in 2015, the Space Data Link Security (SDLS) protocol, providing guidelines to integrate basic security features (i.e., encryption, authentication and authenticated encryption) to the committee's widely used space data link protocols. This standard has been complemented in 2020 by Extended Procedures, increasing the capabilities of the security features provided by the standard with key management and security monitoring services. However, the industry's slow adoption of the standard and the late development of compliant market products are insufficient when faced with the urgency that cybersecurity threats pose to satellite services.

This paper aims to present a framework for the development of security solutions with ease of deployment and security best practices in mind. To provide a solution that can be widely used and swiftly integrated into already deployed systems, compliance with standards is needed. With this aim in mind, a test platform has been developed by the authors to simulate the link between a spacecraft and a ground station using CCSDS protocols with SDLS for the secure transfer of commands and telemetry. This environment provides extensive data logs of security and communication events that occur between the two endpoints and provides tools to experiment with potential attacks on the secure link. The versatility and potential of these tools for improving the security of satellite communication is discussed, and the initial results of the security implementation to a variety of test scenarios are detailed.