Paper ID: 89228
oral

IAF BUSINESSES AND INNOVATION SYMPOSIUM (E6)
Strategic Risk Management for Successful Space & Defence Programmes (4)

Author: Dr. Louis Masson
Cysec SA, Switzerland

SAFEGUARDING SATELLITE COMMUNICATIONS: RISK MANAGEMENT AND MITIGATION STRATEGIES FOR THE DATA LINK LAYER

Abstract

Valuable satellite infrastructure coming from the rapid growth of the space industry has become critical to modern society and governments worldwide, raising the stakes of securing such assets. Increasing global threats and rising conflicts in today's political climate increase further the likelihood of disaster for these irrecoverable assets. Satellites require frequent maintenance and monitoring during the lifetime of their mission: data and commands, exchanged between mission operations and these spacecraft, are transported by transfer frames of the Data Link layer of the Open Systems Interconnection (OSI) model: Telemetry (TM) carries information about a satellite's housekeeping and payload data, while Telecommands (TC) control a satellite's attitude control, propulsion, and mission parameters. Due to open communication standards such as CCSDS TM/TC protocols, the Data Link layer is a uniquely threatened portion of a satellite's communication compounded by the ease of procurement of radiofrequency equipment capable of communicating with satellites. It is only a matter of time before bad actors with sufficient resources and motivation will be able to disrupt these communication channels and imperil the confidentiality, integrity, and authenticity of the satellite's data link and operations. This paper focuses on the risk management of satellite communications occurring on the Data Link layer of the OSI model. A broad scope of threats inherent to this layer of the communication stack will first be discussed: spoofing, Denial of Service (DoS), replay attacks, and sniffing are all potential attack scenarios that can be perpetrated by external actors to a satellite's communication. The vulnerability of satellites in the face of these threats and their consequences will then be explored in various plausible scenarios: orbital assets can be held at ransom, spacecraft with propulsion can be weaponized in orbit, and critical infrastructure can be disrupted by a hostile nation or actor in times of war. Finally, the mitigation techniques to secure satellite communications will be discussed at length with respect to a multitude of initial assumptions regarding a satellite's or a constellation's operations: authentication and encryption can be implemented to minimize the occurrence of attack scenarios identified earlier; security best practices regarding the rekeying of secure links can be put in place to extend the security guarantees of authentication and encryption. Recommendations with regards to the implementation of such practices, notably with the adoption of security standards such as the CCSDS Space Data Link Security (SDLS) protocol will be explored.