55th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Stefano Alberico
Skudo OÜ, Estonia

END-TO-END HARDWARE ENCRYPTION AND PKI FOR CCSDS/SDLS SATELLITE COMMUNICATION

Abstract

In today's world, many essential and critical systems (such as communications, financial services, air transport, weather monitoring, maritime trade and defence) all rely heavily on space infrastructure, including satellites, ground stations and data links. Like any other increasingly digitized critical infrastructure, satellites and other space-based assets (as well as ground based) are vulnerable to cyberattacks. If not contained, these threats could interfere with global economic development and, by extension, international security. In this paper, we propose a modern satellite end-to-end data encryption and authentication method based on the integration of a mature hardware-based cryptography with an updated and extended version of a standard CCSDS space protocol. The core aspects are the integration of a PKI, asymmetric cryptography and digital certificates with a custom extended version of the SDLS protocol (notably originally designed for symmetric encryption only). Every space, ground asset and operator are given a digital identity based on a X.509 digital certificate which is the fundamental element to guarantee a secure mutual end-point authentication. The identity is rooted and managed by a custom Hardware Security Module (HSM) implemented within a single FPGA chip. It is also responsible for all crypto primitives (symmetric, asymmetric and digital signature/verification), key management and storage. Every end-point is in fact provided with one HSM unit which provides also the Root of Trust. The SDLS communication session is initially secured and authenticated via ECDH and then carried on using AES256 and GCM which also allows a secure "Over The Air Re-keying" functionality (OTAR). Such method provides very strong bi-directional authentication and end-to-end hardware encryption allowing secure uplink and downlink satellite communication both for TC (commands sent to the satellites) and TM (data sent to the ground) protocols. We demonstrated a fully functional prototype (developed within a contract for the European Space Agency) with two hardware end-points (one acting as the satellite and one as the ground station) connected via a VHF packet radio modem at 1200 baud. Fully operative SDLS/TC/TM protocol able to send and receive data end-to-end hardware encrypted by the HSM/FPGA chip. In our approach, we demonstrated a viable solution to the problem of providing a strong end-point authentication combined with end-to-end hardware-based encryption. The next steps are about improving the keys/certificates management functions, integrate the SDLS/PKI handling inside the FPGA chip and replace the ECDH/Ed25519 with Post Quantum Cryptography (PQC) algorithms.