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

Author: Mr. Jens Freymuth
Technische Universität Berlin, Germany

Mr. Philipp Wüstenberg
TU Berlin, Germany
Mr. José Manuel Diez
Technische Universität Berlin, Germany
Mr. Thee Vanichangkul
Technische Universität Berlin, Germany
Prof. Enrico Stoll
TU Berlin, Germany
Mr. Philipp Kampermann
German Space Agency, Germany
Dr. Siegfried Voigt
German Aerospace Center (DLR), Germany

ADVANCING CYBERSECURITY FOR SATELLITE COMMUNICATIONS IN THE QUANTUM COMPUTING ERA

Abstract

Satellite-based services are an integral building block for our modern societies. From global communication networks to environmental monitoring systems or the resilience of critical infrastructure. This dependency results in heightened cybersecurity risks, emphasizing the necessity for satellite security measures and robust communication systems. Additionally, the rise of quantum computing increases these security risks significantly, especially for public key cryptography.

Addressing these challenges, the RACCOON project of the Technische Universität (TU) Berlin funded by the German Space Agency (DLR) was initiated in 2022. The project aims to develop an intelligent and robust RF transceiver, designed to autonomously scan for secure communication channels. The transceiver facilitates, combined with a powerful computational unit, the secure transmission of symmetric keys. Together with its partners, particularly Vattenfall and the German Association of Energy and Water Industries (BDEW), the RACCOON system will demonstrate an encrypted communication between an energy provider and a remote power plant (e.g. offshore wind turbine). This application underscores the system's capacity to ensure data integrity across potentially compromised networks to increase the resilience of satellite-based communication services in crisis situations.

During the development of the RACCOON payload the partners identified the lack of a publicly accessible, security-centric satellite operating system as a significant vulnerability. The project team develops a comprehensive solution, called the RACCOON Operating System (RACCOON OS), that integrates state-of-the-art security features and advanced resilience against cyber attacks into a into a compact, powerful and open-source satellite operating system.

In summary the RACCOON project aims to advance robust satellite communications, offering a novel framework to safeguard differnt fields of application such as critical infrastructure against emerging threats related to quantum computing. This paper will introduce the current status of the RACCOON project, includes insights into the development and testing of the Engineering Qualification Model (EQM) of the satellite payload and the inaugural release of the RACCOON OS. Additionally, common attack vectors, lessons learned and the outlook into the next project phase will be presented. It is planned to realize a practical in-orbit demonstration, to validate the operational capabilities of the RACCOON system. Additionally, the upcoming CyBEEsat mission, which acts as a testbed, will provide empirical data to inform further development.