Paper ID: 101791
oral

58th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Mr. Philipp Wüstenberg
TU Berlin, Germany

Mr. José Manuel Diez
Technische Universität Berlin, Germany
Mr. Jens Freymuth
Technische Universität Berlin, Germany
Mr. Fabian Krech
Technische Universität Berlin, Germany

RACCOON OS - TOWARDS A CYBER SECURE OPEN-SOURCE OPERATING SYSTEM FOR SPACE APPLICATIONS

Abstract

Due to the sensitive nature of modern small satellite missions, a robust software infrastructure is essential to protect against threats such as memory leaks, remote code execution, and the risk of satellite hijacking. Even if a compromised satellite does not contain sensitive data, it could be manipulated to endanger other critical space assets. This includes using thrusters for intentional collisions or leveraging differential drag to alter orbital trajectories, posing significant security risks to high-value satellites. Many existing solutions do not sufficiently address these critical security challenges. RACCOON OS fills this gap, ensuring comprehensive protection and cyber resilience in space applications.

RACCOON OS is an initiative focused on developing a cyber-secure, open-source operating system tailored for space applications. Building on a robust Linux-based framework, RACCOON OS integrates modern access controls and advanced security measures to safeguard satellite software against emerging cyber threats. Standard space protocols (ECSS, CCSDS, PUS) are implemented in memory-safe programming languages like Rust, ensuring high reliability and security from the ground up. This paper will provide a detailed description of the current state of the implemented solutions, outlining their capabilities, limitations, and areas for future improvement.

In collaboration with the Helmholtz Center for Information Security (CISPA), the Firmware Security group at Ruhr University Bochum (RUB), and the Chair of Space Technology and the Chair of Security on Telecommunications at TU Berlin, this initiative brings together leading expertise in satellite communications and cybersecurity. Other companies, institutes, projects or individuals are invited to join this initiative, either as users providing feedback, bug reports, and feature requests, or as contributors actively shaping and improving RACCOON OS.

Additionally to the preliminary results of the RACCOON OS development, this publication will outline the the design methodology, decision-making process and key architectural considerations that guided its development. Furthermore, it will provide insights into the next development steps and future plans, along with information regarding the currently planned missions where RACCOON OS will be deployed. By providing insights into the project's technical and strategic choices, we aim to foster collaboration and invite future partners and contributors to join in advancing a secure, open-source future for space applications. Additionally, this publication will include details on existing collaborations and outline future collaboration plans to further strengthen the project's impact and outreach.