Paper ID: 91201
oral
student

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

Author: Mr. Nicolò Boschetti
Cornell University, United States, nb624@cornell.edu

Prof. Gregory Falco
Cornell University, United States, gjf24@cornell.edu

TOWARDS SECURE-BY-DESIGN SPACE MISSIONS: SPACE SYSTEMS DECOMPOSITION TO ENABLE MISSION-WIDE CYBERSECURITY PRINCIPLES

Abstract

Cyberattacks are increasingly targeting space systems, making cybersecurity a more critical concern than ever. Despite the critical nature of space infrastructure, there is a lack of space industry-wide cybersecurity technical standards. Existing guidance commonly does not identify security as a crucial component of a space mission's preliminary design stages. In contrast, the secure-by-design approach can enforce security measures in the early phases of space mission development. The main limitation of this approach is its challenging application to the vast diversity of missions; in fact, the poor applicability of security principles to the unique characteristics of each mission would make this effort vain or counter-productive. This paper will propose a space mission decomposition framework as the enabler of modular secure-by-design principles holistically applicable to heterogeneous space missions.

This paper will highlight existing gaps in the technical literature and relate them to the different building blocks of a space mission. This will set the basis for decomposing space missions into segments, components, functions, and subcomponents. Conceptualizing the space mission as a system-of-systems (SoS), the study will propose an identification framework for the components and subcomponents of the space, link, ground, user segments, and integration layer. The decomposition methodology will serve as the foundation for analyzing the cyber attack surface of the subcomponents. The result will be an architectural and security framework informing secure-by-design principles for designing secure subcomponents of space missions with different security requirements.

The paper will present the results of the decomposition effort for each segment and layer of a generic space mission. In addition, through an example, we will demonstrate the role of this method in identifying the attack surface of a specific subcomponent like the flight software. The attack surface of different iterations of this subcomponent, each with different cybersecurity weaknesses, will be identified and presented. This example will then offer a set of secure-by-design "shall statements" applicable to the design and integration of that specific subcomponent into a space mission.

This paper, authored by the leaders of the IEEE SA International Technical Standard for Space System Cybersecurity (Working Group P3349), also seeks to describe how this framework is being developed as a constitutive element of this international cybersecurity standardization effort. Our methodology and this paper's contributions can constitute a starting point for the space cybersecurity community and policymakers aiming to develop security requirements and frameworks for space missions.