54th IAA SYMPOSIUM ON SAFETY, QUALITY AND KNOWLEDGE MANAGEMENT IN SPACE ACTIVITIES (D5)
Cybersecurity in space systems, risks and countermeasures (4)

Author: Prof. Klaus Schilling
University Wuerzburg, Germany

Prof.Dr. Alexandra Dmitrienko
University Wuerzburg, Germany

INCREASING SECURITY IN SATELLITE NETWORKS

Abstract

Current mega-constellations for satellite communication networks, but also critical infrastructures in GNSS raise new challenging security and safety requirements. Similar to many on-Earth systems (like the Internet), the satellite technologies initially developed with functional requirements as a primary concern, while security objectives received second priority. Today's satellite systems do not employ elaborate security mechanisms similar to on-Earth networks and systems, as the deployment of security mechanisms requires additional resources, which often deems too costly and unjustified given the absence of in-space cyber-threats. However, due to the appearance of cost-effective cloud-based ground stations for satellite control and improved accessibility of satellite launch, the typical barriers of cost are lowered for adversaries, and they may find it appealing to gain unauthorized access to the provided services (and monetizing it), or taking control over satellites and demanding ransom from their service providers. It is likely that the attackers will be able to apply their tech knowledge collected on-Earth for attacking satellite systems since they feature similar Internet protocol-based technologies inside CCSDS standards. Hence, we face the perspective to deal with skilled attackers, while often even simple security practices such as encrypted and integrity-protected communication and software patching are not applied.

In this contribution, we aim to transfer and adapt terrestrial countermeasures to cyber-attacks in-space towards securing satellite systems further. This paper performs an analysis of potential threats and formulates security requirements for satellite systems. A balanced trade-off between required resources for security and achieved benefits will be addressed. Notably, in-space security threats are different from those relevant for on-Earth systems – for instance, an attacker is likely to attack communication links, but unlikely to have physical access to satellite's hardware and, e.g., extract cryptographic material. On another hand, software attacks, such as exploitation of software vulnerabilities, is a valid attack vector, since satellites run software that may have similar vulnerabilities as on-Earth systems. To identify relevant threats, we define various attacker models targeting common commercial satellite applications, analyze potential attack vectors, formulate security objectives and requirements, and make recommendations on how to fulfill them.