Paper ID: 60825
oral

IAF SYMPOSIUM ON SPACE SECURITY (E9)
Cyber-security threats to space missions and countermeasures to address them (2.D5.4)

Author: Prof.Dr. Emiliano Casalicchio
Sapienza University of Rome, Italy

Prof. Paolo Gaudenzi
Sapienza University of Rome, Italy
Prof. Luigi Vincenzo Mancini
Sapienza University of Rome, Italy

KEYNOTE: CRISES: CYBERSECURITY FOR SMALL-SATELLITE ECOSYSTEM - STATE-OF-THE-ART AND OPEN CHALLENGE

Abstract

In the next decade, about 50 thousands of small-satellites will orbit around the earth, mostly as element of large constellations. The small-satellite ecosystem includes satellites with a wet mass of less than 500Kg, like nanosatellites (1 - 10 Kg) and picosatellites (0.1 - 1kg). No matter what the size of the satellite, the technical and economical feasibility of the space system is requiring low costs for the design, manufacturing, launch, operations of such a large number of satellites. The purpose of the missions of these new kind space systems is typically a commercial one and clients and stakeholders have different objectives, from bringing internet access to remote corners of the globe to monitoring the environment and improving global navigation systems. Cyber security issues are a very critical topic for the new constellations since they may not only put in jeopardy the service but even allow the loss of control of the asset that would be eventually used for different purposes by different users.

The scope of hacking a small-satellite or an entire constellation of small-satellites include: rendered the satellite-constellation useless, making some services unavailable (to disrupt ground applications), hold satellites for ransom, stealing sensitive information, or using small-satellite as physical weapons to harm government or military owned satellites.

In commercial small-satellite, the use of COTS components, the limited processing capability available on board due to the light payload, and the open architecture introduce new vulnerabilities to cyber attacks. This is a completely new scenario. Indeed, traditional satellites operated by government or military agencies are produced ad-hoc, typically use dedicated high quality hardware and software components and keep secret the design and implementation details. So far, hacking of gov/mil satellites required the involvement of insider and espionage to get knowledge about the technologies used and their vulnerabilities. Today, hacking of small-satellites is not so different from hacking an IoT device, a SCADA or industrial control system [1]. Today hackers could leverage the on-board software vulnerabilities and communication protocol vulnerabilities in addition to the vulnerabilities offered by the traditional attack surface (control and communication ground stations, data links, tracking and control links).

Moreover, the lack of cybersecurity standards and regulations for commercial satellites, in the EU and internationally, exacerbate the security problem [2].

This paper, firstly provides a review of cyber-threats in the small-satellite ecosystem, with a focus on data links, tracking and control links, and the on-board software. Then, it analyzes cutting-edge computer

[1] D.E. Cunningham et al, Towards Effective Cybersecurity for Modular, Open Architecture Satellite Systems, AIAA/USU Conference on Small Satellite, 2016

[2] D.P. Fidler, Cybersecurity and the New Era of Space Activities, 2018 https://www.repository.law.indiana.edu/facpub/2665

security techniques that can be used to reduce the effects of cyberattacks, and finally it provides an outlook of open challenges.