17th International Conference on Space Operations, Dubai, United Arab Emirates, 6 - 10 March 2023.

SpaceOps-2023, ID # 125

The Space cybersecurity Framework : The OPS SAT Red Team approach

Jamel Metmati

[a] *Department of Cyber,* djamel.memati@thalesgroup.com

Abstract

The commercial opening of Space through private actors supported by states or not able the possibility put the space networks face to the effects of robustness to the service. To ensure the full delivery of a service, the hardening need to be improve by the networks Team : blue, purpose, and above all the red team. The work is supported by the Defence security certified in Space for the Space networks assessment to put in place a programme to evaluate and to test Space networks and improve their resilience to manage the mass-market application in New Space. And the offensive security certified in Space exist to think about the scenatios potentially applicable to disturb the functionalities of assets in Space delivering services for the ground segment. To demonstrate the capabilities of Space Red team, OPS-SAT is small satellite allowing to show and to improve mission control features thanks to an experimental computer on board.

Keywords: OPS-SAT, New Space, Red-Team, Scenarios, GPS

Acronyms/Abbreviations :
TM/TC : Telemetry Command and Control
DVB : Digital Video Broadcasting
NORAD : North American Aerospace Defense Command
SNR : Software Network Radio
SoT: Space of Things
NMEA: National Marine Electronics Association
ADCS: Altitude Determination and Control System
CCSDS: Consultative Committee for Space data systems
SMILE: Special Mission Infrastructure Lab Environment
SW : Software

1-Introduction

The objectives of the work is to present the capacity to use Space assets to ensure the qualification, the operationality, the maintenance of the Space networks in the New Space context. It holds on the existing means and the international frameworks in information system to propose a framework applicable for operational team on the ground.

2. Material and methods

The material is a platform with a test satellite on low orbit and a platform on the ground. The method consist of the simulation to connect the assets on the ground to Space.

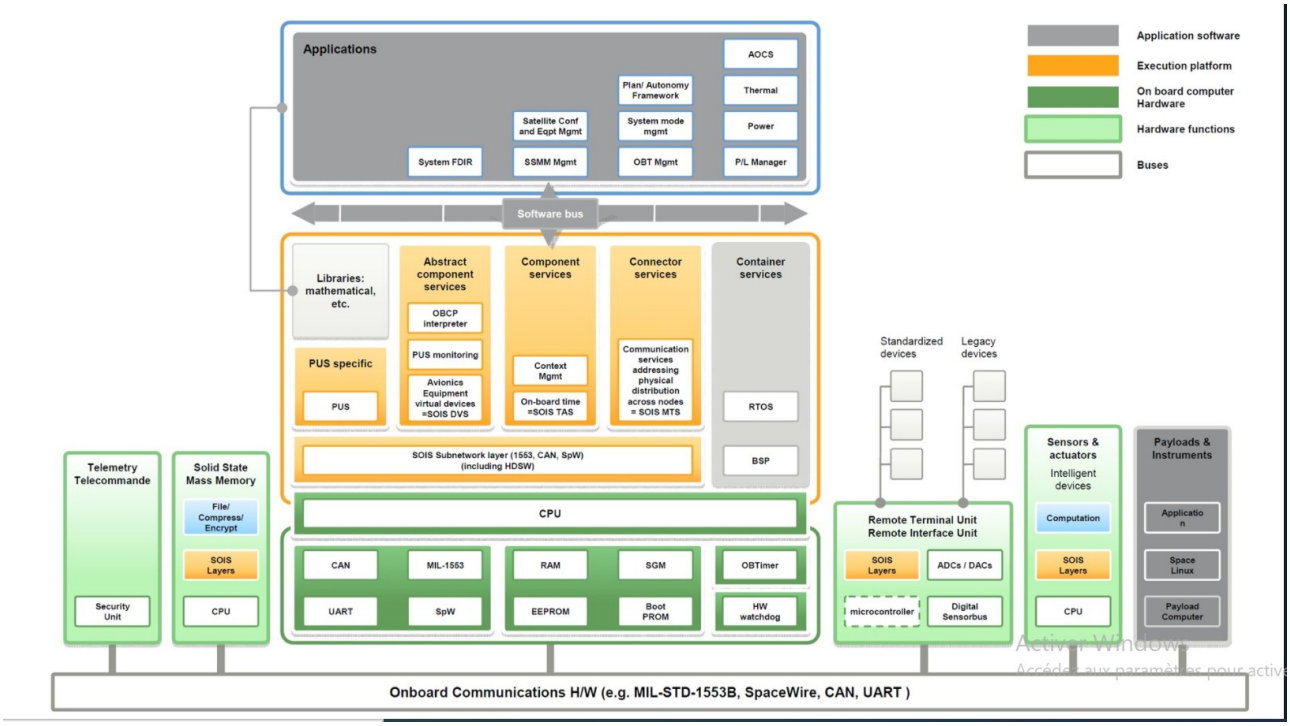

Figure 1 : Architecture Data on Board

3. Theory and calculation

The tools for Space Red team needs to mix the classical tools for data dissemination on the terrestrial networks with the capacity to test the OPS-SAT signal transmission and communication between the Space to the ground. The critical one is the telemetry (TM) encoder which collects the Telemetry packets from different sources (processing, data storage, essential telemetry, payload), and the assembler fo the telemetry transfer frames and the sends to the TM/TC transceiver to be downloaded to the ground station.

The framework [1] closer to be used can be the SoT applicable which can be applied to the satellites like OPS-SAT. The methodologies for the defences and the attacks are applicable thanks to the gold path. It means the way to advance in the defence of the network. The path is never written in advance. Nevertheless, the Space framework insists on the network behaviour understanding to explore well the functionalities to make him more robust.

The steps are to make the transmission and communication links understandable. The equipments, the protocols, the data are the core of networks named under the architecture. Then, the configuration elements provide the functionalities of the networks and the purpose of the applications. This phase calls the system prelimenary design to do the exploration test. The second phase is to plan with the customer the equipments that will be tested to avoid a degradation of the OPS-SAT. The exploration test can be done in a laboratory by simulation by software or by connecting the payload module with others equipments. The third phase is close to exploration path known by the pentesters [2] : scan, detection, deliver by the means to move, and the exploitation by the exploration. Its phase introduces the tools to response with the specificity of OPS-SAT.

The points for the tools is to understand what is the OPS-SAT safety and the security in Space. There are measures to be taken to secure the payload and the capacity of OPS-SAT to work in a harsh context.

The way described on below can be applied for the laboratory test to the payload module functionalities. An another way should be to built an information and communication center with satellite ground station able to be connecting to OPS-SAT in low orbit with the satellites zombies, the satellites scanner, the satellite radar, the satellite relay for the manoeuver the zombies one to be closer the satellites target.

The tools to scan shall be supported by the software with radio materials. The SIGINT OS is useful to orient the scan to radio wave. The linux distribution can be installed with DVB and the Kali linux VMWare for the scan tool like wireshark DVB. The plus of the installation is to use radio amateur materials. Further, the best is to built an information and communication center with satellite ground station.

The tools to detect shall be the materials to catch the frequency of the OPS-SAT, in understanding the transmission and communication frame, its encoded and the moment where the satellite is passing overhead detection point choosen. The link like n2yo.com provide the computation of the path for any satellites launched.
The types of the satellites [3] must be understood through its NORAD ID, its latitute, its longitude, its altitude, its speed, its azimuth, its elevation, its right ascension, its declinaison. A Sms alert can provide the timing path for the detection. Then, these requirements shall be associated with the line budget of the satellite to get the opportunities of data exploration when the signal is enough high.
Indeed, the scan must determined the critical link with the satellite through the availability of power at the ground station, the power at the satellite sensitivity of the receiver SNR at the receiver reception level in taking account the interferences. The means to visualize the link can be provided by the satellite counter, the spectral analyzer, the spectrogram. It can be completed by real time analyzer or a scanner.
The tools to exploit shall be the kali linux software to make the connection with the interface of computer on board thanks to the signal incoming. At last, the watchdog software is useful tool for the payload system to check all parameters of the on-board computer : test process table, memory usage, network interface traffic between the module, temperature, IP adressing. It gets the option to shutdown the processing on board in case of data anomalies in regard of the requirements of nominal subsystems functionalities. The point can be monitored by C+ or Python API code on below to get the logs of satellites payload from the events choosen avoiding the infinite loop if the memory is corrupted.

```
def __repr__(self):
return ("<%(class_name)s: event_type=%(event_type)s,
      " "src_path=%(src_path)r, "
      "is_directory=%(is_directory)s>" )
       % (dict(
              class_name=self.__class__.__name__,
              event_type=self.event_type,
              src_path=self.src_path,
              is_directory=self.is_directory)
```

4. Results

4.1-Scenarios one Space Red Team

The technical coordinator of the Space Red Team provides a scenario in which an OPS-SAT can be disturbed during the operations phases between 1 to 2 years, and a scenario after the OPS-SAT launch in a low orbit context.
The launch early and operational period should be considered by the platform to test the communication and transmission link between the mission planning operation and the experimenter interface.
The targets have been identified and the path to potential attack by failure or by external data has been described against the main services of OPS SAT : the camera service, the GPS service, the ADCS service, the Software-defined Radio service, the Optical Data Receiver service, the Generic Device. The Camera service provides common operations for interfacing with cameras on-board of a satellite platform. The GPS service provides common operations to receive data from a GPS receptor.
The service shall provide the possibility to read directly the data format NMEA output coming from the receptor, an operation to get the last known position transmitted by the GPS, a way to manage zone proximity alerts that can be set and defined by the user of the service. The Altitude Determination Control System service provides operations to operate an ADCS on-board of the OPS-SAT. The Software-defined Radio provides operations to configure and receive a stream of data. The Optical Data Receiver allows a consumer to receive a stream of data. The Generic Device service allows a consumer to send and receive data in a generic way from any device available in the platform. The analysis team provide the first consequences linked with the degradation of these services. To counter the vulnerability of the path, the Space Red Team provides information to help the blue team to detect, mitigate and prevent the attack. Two types of threats have been detected by the team.
The first is the platform test on the ground with the process to maintain the OPS-SAT and to validate the sofware design. During the commissioning phase of the mission, the operational capability of all bus subsystems and in-orbit validation shall be checked : ADCS, S-band high speed communication chain with CCSDS engine.
The OPS-SAT operations phase includes planning, execution, evaluation, and exploitation processes of experiments during one or two years. The point is viewed as critical because some contractors are included in the information

process and the version of software must be compliance with integrity criterias. The environment of OPS-SAT development use a workstation connected with a experiment server directly or via Internet to store experimentes delivrables through information control document for the project in which there are procedures, meta-data, executables. The outcome experimentes store logs, results, telemetry data. To simulate the mission planning and operating, the experiment server is linked with two workstations to represent the ground segment and the space segment. The first workstation station concerns the flatsat bed test for integration and test, flight software, flight operations. The second workstation gets a RF link with the OPS-SAT payload to test the processing platform between : the antenna inbound/outbound for telemetry, the on-board computer, the store data experiment, the others peripherals like sensors.
The sofware used pays attention because to built the platform, the explorers note the configuration following : the experimenter uploads the VM image(s) to a central VM manager. The VM manager is a repository of VM configurations, kept under versioning and with a description, entered by the experimenter. And the payload sytems run with Angström embedded linux from IntelFPGA with the vulnerability following : The server is configured to use password only authentication not cryptographic keys, however the firmware image contains an RSA host-key for the server. An attacker can exploit this vulnerability to gain root access to the Angstrom Linux operating system and modify any binaries or configuration files in the firmware. Moreover, the VM manager provide a corrupted version allowing an elevation of privileges.
The experimental ground segment is installed in the SMILE environment with a ESOC-1 radio amateur facility antenna which supports S-Band up and down links, X-Band down links, VHF (Very High Frequency), UHF (Ultra High Frequency) up and downlink and amateur S-Band downlink. The experimenter may run validation and verification tests on it. Each experiment is assigned a unique Application Process ID (APID), to be able to route Telemetry control and Telemetry mission from the experiment.
The experiment is uploaded as software images containing executable JAR files, linux code, kernel code, or FPGA firmware (raw binary files). However, the team shows the wrong sequence in APID in the real-time data process. A unique APID for each onboard SW experiment. This uniquely identifies the source of a TM packet and the destination of a TC packet. This uniquely identifies the source of a command packet.
The experimental ground segment can send commands to this APID and to the APID of the peripherals but neither to other experiment nor any other system. However a backdoor in the software shows the possibility to send a critical command for software image uploads and satellite reset.

4.2-Scenario two Space Red Team
The second scenario is linked with the OPS-SAT in Space with data from NMEA message transmitted between the ground and the low orbit. The scenario shows data NMEA from GPS system in the OPS SAT thanks to wireshark DVB for the gelocalisation tag antenna and data inbound and outbound. The data on below gets some information as GP for GPS, the type of NMEA message for GGA, the timestamp value, the latitude, the longitude, the location value, (1= GPS fix, 2=DGPS fix, 3=PPS fix, 4=Real Time Kinematic, 5=Float RTK, 6=Estimated, 7=Manual input mode, 8= Simulation mode), the satellites number, the altitude of OPS-SAT :

$GPGGA,201500.00,4507.7409876,S,78744.6456786,
W,4,1,1.00,500,M

It can be completed by the orbital parameters of OPS SAT providing by the launch early operational phase on below by social engineering or by cognitive attack in the process of data flow within the organization. The cognitive attack means the capacity to by pass the brains functionalities in the context of information expected or unexpected.

NORAD	78078
COSPAR designation	2000-066-AE
Inclination (degree)	97.765
RAAN	92.182
Eccentricity	0.0063803
ARGP	9.709
Orbit per day	14.77396564
Period	1h 56m 28s (97.47)
Semi-major axis	8 016 km
Perigee x apogee	523 x 642 km
Drag factor	0.000272870 1/ER
Mean Anomaly	380.449

Figure 2 : Main OPS SAT parameters

After, the antenna geolocation tag shows the following manner thanks to filter based on GPS with the information following :

((ppi_gps.lon <= -155.01) && (ppi_gps.lon >= -155.03) && (ppi_gps.lat >= 19.01) && (ppi_gps.lat <= 19.03))

12.2.

Another filter by omni-directional antenna where the packet was received with a signal value of > - 75Db :

(ppi_antenna.horizbw == 360) && (radiotap.dbm_antsignal > -75)

The point is the location of the OPS SAT can be determined with its path with the power used to transmitted the data between the ground segment and the OPS-SAT. Commonly, the S-band, UHF and X-band provide the carrier wave to the data. The degradation is able to be done with enough power from stations in the ground. From Space, others OPS-SAT or satellites could be able to produce enough power by calibration manoeuver close to the OPS-SAT target. The data packets for telemetry, telemetry and telecommand is the parallel input of scan space networks. The health of a satellite is determined by the telemetry. The telemetry data transmited to the ground stations is critical also for the maneuvers of the OPS-SAT. The beacon packet between Space to ground shows the clocks and the timers, the payload status, the communication status, the battery status.
The amateur radio materials is useful to show these datas. From the ground, a mini information and communication center could be a wifi grid mesh antenna 100x60cm on tripod or parabolic one, a TV MMDS downconvertor on 2.1/2.3 GHz for S-Band with Airspy, SPF5189Z LNAs and SDR Hack RF. As said, the x-Band need more power with huge parabolic antenna. This center connecting with others OPS-SAT on orbit can display the data incoming from Space.

5.Discussions

5.1-The Space Red team organization

The Space framework delivers the certification to use Space networks for the application through the ground segment and its connectivity with the other networks. It helps an entity to assess its protection, detection and response capabilities to the networks between the ground and the Space segment to the end-users. The objectives of the Space framework [4] has the following core objectives :

1. to enhance the cyber resilience of Space networks,
2. to standardise and to harmonise the way entities perform intelligence-led red team tests across the Space compagny, allowing each jurisdiction a degree of flexibility to adapt the framework according to its specificities,
3. to provide guidance to Space compagny on how they might establish, implement and manage this form of testing on their OPS-SAT,
4. to show by the scenarios the work of Space team,
5. to provide the way to robust the networks by data exploration.

The Space Red team OPS-SAT provides an overview of networks, and how it will be implemented across the ground segment and on spacecraft, with details of the key phases, the activities, the deliverables and the interactions involved in a test with the tools associated. The Space Red team shall be defined by a group of people able to explore the space networks to ensure the robustness of data flow to the ground segment. The Space red team is organized following the tasks of the networks and the functionalities of the OPS-SAT in Space.
In the context of New Space, the satellite are smaller getting on board computer under the proof of concept "Computer in Space" [5]. The payload entry is the antenna and the computer on board managed the others modules functionalities. It depends on the nature of the satellite.
The antenna is based on a frequency and its size provides the transmission capacity. At last, the orbit of the payload gives the position expected and the energy to be use to up-link and down link signal. The signal processing between the ground to Space, through the line of budget study, provides a visualization of the transmission. Then, the exchange of data contents the configuration, the parameters, the functionalities like the terrestrial networks [6]. With these features, a Space Red team shall be adapted in its organization. An framework should be divided in several groups:

1. The signal team for the ground to Space,
2. The network team for the terrestrial network including the ground segment and the infrastructure,
3. The analysis team in charge of study data from the signal team,
4. The joint staff in charge of the path of exploration in the Space networks,
5. The explorers team in charge to realize the exploration.
6. The documentary team in charge of the archiving the exploration campaign for the explorer and the technical coordinator.

The explorer team provide in the same times feed back to the analysis team when the exploration is not anymore possible. The technical coordinator is in charge of the support the information flow to improve the quality of the exploration and to identify by risk analysis, with the figure 1, the critical subsystem for the OPS SAT.

6. Conclusions

The Space Red team combines the full capacity of the human technology with a framework able to ensure the operations of application. And above all, the team support the safety and the security in Space for the future missions on orbit and further.

References

List of references

Reference to a book:
[1] G. Falco and N. Boschetti, "A security risk taxonomy for commercial space missions," in ASCEND 2021, 2021, p. 4241.
[2] Malware: Fighting Malicious Code. Skoudis E., Zeltser L., 2003.
[3] Falco, G.: Cybersecurity principles for space systems. J. Aerosp. Inf. Syst. 16(2), 61–70 (2019).
[4] Space mission analysis and design. Space technology library; v.8, Microcosm ; Kluwer Academic, Torrance, Calif.:Dordrecht; London, 3rd ed./edited by james r. wertz and wiley j. larson. Edn. (1999).

Reference to a journal publication:
[5] Zimmerman, R., Doan, D., Leung, L., Mason, J., Parsons, N., Shahid, K.: Commissioning the world's biggest satellite constellation. In: 31st Annual AIAA/USU Conference on Small Satellites. No. SSC17-X-03 in Year in Review (2017). https:// digitalcommons.usu.edu/smallsat/2017/all2017/. Accessed 17 Apr 2019.

Reference to a conference/congress paper:
[6] Kyle Colton, B.K.: Supporting the Flock: Building a Ground Station Network for Autonomy and Reliability. In: 30th Annual AIAA/USU Conference on Small Satellites. No. SSC16–IX–05 (2016)