

Simulating and Observing Satellite Threats: A Monitoring-Aware Cyber Range for Satellite Security Training

Lorenzo Bracciale **Matteo Ciccaglione** Alessandro Amici
Fabio Patrone Nour Badini Mario Marchese Andrea Detti
Daniel Xhakalliu Giuseppe Bianchi Michele Luglio
Luca Fiscariello Cesare Roseti Arianna Miraval

University of Rome Tor Vergata, National Inter-University Consortium for
Telecommunications

November 6, 2025

The Vacuum of Space Cybersecurity

"A technology too
advanced
to compromise"
(Iridium)



¹ (Gregory Falco. "The vacuum of space cyber security". In: *2018 AIAA SPACE and Astronautics Forum and Exposition*. Reston, Virginia: American Institute of Aeronautics and Astronautics, Sept. 2018)

The myth of inaccessibility is falling down

AWS Ground Station

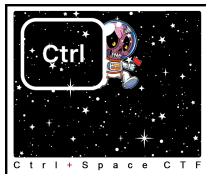
Easily control satellites and ingest data with fully managed Ground Station as a Service

Get started with AWS Ground Station

GaaS



SDR



CTF

WikiLeaks Leaks News About Partners

page | discuss | view source

Iridium Security

Release date
April 9, 2008

Download
[File](#) | [Torrent](#) | [Magnet](#)

Further information

Context
[United States](#)
[Company](#)
[Iridium](#)

Primary language
[English](#)

File size in bytes
237318

File type information
PDF document, version 1.4

Cryptographic identity
SHA256 c1b3adcf2d88ebb6bd13e4a05c66de10153075007a7543c60134dafc

Description (as provided by our source)
Confidential presentation on Iridium Security

1. not released before to my knowledge, please verify
2. describes a security standard for satellite communications that is flawed (x
3. anyone interested in technology and bad designs, users of Iridium who thir
4. contact mr wigglesworth?
5. for general informational purposes
6. no

Levels of Enlightenment in Satellite Cybersecurity

**IGNORE
CYBERSECURITY**



**USE SECURITY
BY OBSCURITY**



**IMPLEMENT
BASIC ENCRYPTION**



**BUILD AN OPEN,
TESTABLE CYBER
RANGE FOR
SATELLITES**



Filling the vacuum: OpenSatRange

- CyberRange for Satellite Systems



+



Intuitive Graphic Interface

User Activity Monitoring System

KYPO

Cyber Range Platform

KEYCLOAK

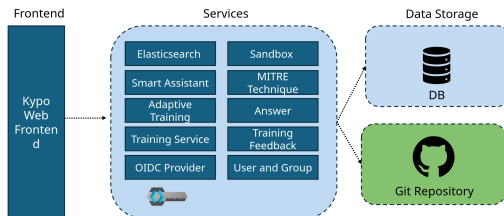
Keycloak Integration

Git

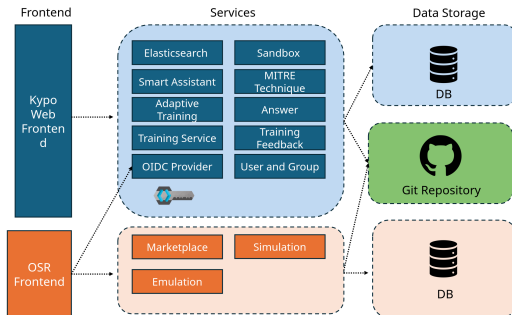
GitHub

Git Repository for Sandbox Management

OSR Architecture



OSR Architecture



Satellite Simulation

Satellite

GEO Options

[Add New GEO Node](#)

LEO options

№ of sat per orbita

Altitude (km)

Inclination (deg)

Eccentricity

Arg of Perigee (deg)

Antenna Gain (dBi)

Antenna Diameter (m)

ERP Density (dBW/MHz)

Load TLE file

[Choose](#) [Upload](#)

No file chosen

User

Stationary Options

[Add New Stationary Node](#)

Airplane options

[Add New Airplane Node](#)

Pedestrian options

[Add New Pedestrian Node](#)

Car options

[Add New Car Node](#)

Gateway

[Add New Gateway](#)

Environment

Simulation Duration

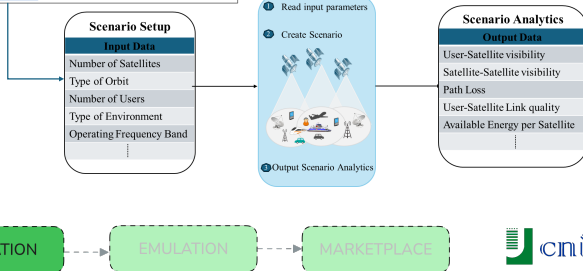
Scenario Type ☒ Green Urban ☐ Urban ☐ Suburban ☐ Rural

Operating Band ☒ S-Band ☐ Ka-Band

RB_Bandwidth (MHz)

Shadowing ☒ Disabled ☐ Enabled

Title



Satellite Simulation

**Different Mobility Models
and Coordinate Systems**

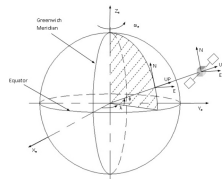
**Higher Distance-Higher
Delays**

Different Antenna Models

Different Channel Model

ns-3
Network Simulator

Figure 2 ECEF and navigation frames.



| Elevation | S-band | | | Ka-band | | |
|-----------|---|---|---------|---|---|---------|
| | LOS $\sigma_{\text{LOS}} \text{ (dB)}$ | NLOS $\sigma_{\text{NLOS}} \text{ (dB)}$ | CL (dB) | LOS $\sigma_{\text{LOS}} \text{ (dB)}$ | NLOS $\sigma_{\text{NLOS}} \text{ (dB)}$ | CL (dB) |
| 10° | 3.5 | 15.5 | 34.5 | 2.9 | 17.1 | 44.3 |
| 20° | 3.4 | 13.9 | 30.9 | 2.4 | 17.1 | 39.9 |
| 30° | 2.8 | 12.4 | 26.0 | 2.7 | 16.8 | 37.5 |
| 40° | 3.0 | 11.7 | 27.7 | 2.4 | 14.8 | 36.4 |
| 50° | 3.1 | 10.6 | 26.8 | 2.4 | 14.2 | 34.8 |
| 60° | 2.7 | 10.5 | 26.2 | 2.7 | 12.6 | 33.8 |
| 70° | 2.5 | 10.1 | 25.8 | 2.8 | 12.1 | 33.3 |
| 80° | 2.3 | 9.2 | 25.5 | 2.8 | 12.3 | 33.0 |
| 90° | 1.2 | 9.2 | 25.5 | 0.8 | 12.3 | 32.9 |

SIMULATION

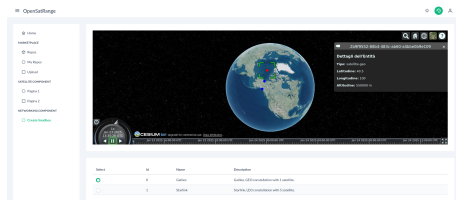
EMULATION

MARKETPLACE

Satellite Emulation

- GEO:

- Each network segment is modeled as an OpenStack virtual network;
- Each entity is represented by a dedicated virtual machine with an OpenSAND.



- LEO:

- The constellation is implemented within a single virtual machine;
- Each satellite is modeled as a separate network namespace;
- SDN is used for network control.



Marketplace

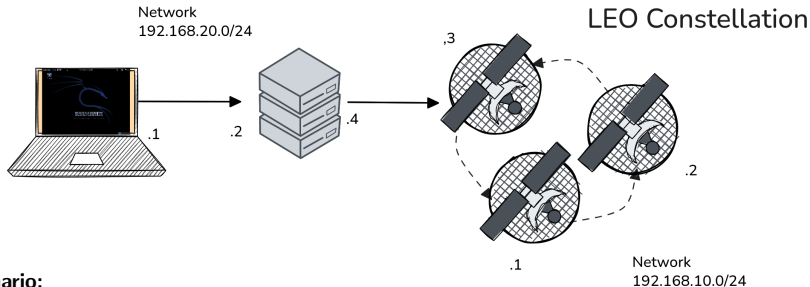
The screenshot displays the OpenSatRange Marketplace interface. On the left is a sidebar with navigation links: Home, Profile, and a section for MARKETPLACE containing Repos, My Repos, and Upload. Below this are sections for SATELLITE COMPONENT (Simulation) and NETWORKING COMPONENT (Pagina 1, Pagina 2). The main area features a grid of project cards, each with an author, title, description, star rating, and buttons for Details and Copy. The projects shown are:

- Quantum Sandbox** by code_legend (20 stars): A playground for quantum computing algorithms.
- AI Emulator** by code_legend (73 stars): Simulates neural networks in various configurations.
- Sim Space** by code_legend (22 stars): A space simulation environment.
- Nano Sandbox** by code_legend (86 stars): Experimenting with nanotechnology models.
- Sim City** by dev_dreamer (49 stars): A city simulation project for urban planning.
- Meta Emulation** by dev_dreamer (53 stars): Emulates meta-level AI reasoning.
- Cyber Sandbox** by dev_dreamer (47 stars):
- new-sandbox** by ploreti (43 stars):
- original** by ploreti (3 stars):



Tampering with the firmware of a satellite

LEO (Low Earth Orbit)

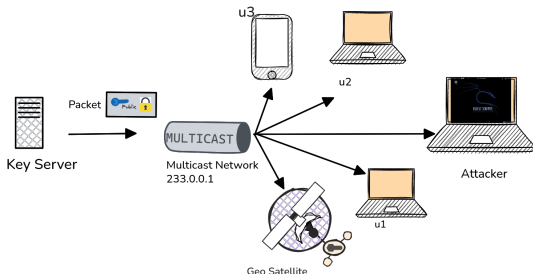


Scenario:

- The student will identify a web vulnerability in the Ground Station system.
- Exploiting this flaw, they will gain privileged access to the control machine.
- They will initiate a firmware update procedure using a custom payload, resulting in a deliberate satellite outage.

Intercept and decrypt a satellite communication

GEO (Geostationary Earth Orbit)

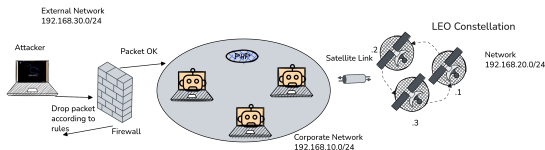


Scenario:

- The student intercepts satellite messages transmitted in CCSDS format.
- These messages include public keys and encrypted payloads.
- By analyzing the public keys, the student performs a Common Factor Attack to retrieve the corresponding private keys and decrypt the communication.

Launch a DDoS attack against a LEO satellite constellation

LEO (Low Earth Orbit)



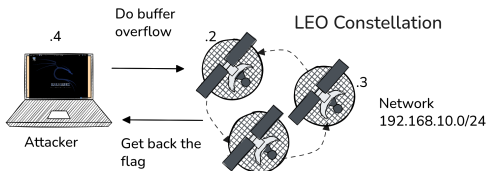
Scenario²:

- The student compromises machines within a corporate network that has access to the satellite service, building a custom botnet.
- They develop a Python-based C2 (Command and Control) software to coordinate the botnet.
- The botnet is then used to launch a distributed denial-of-service (DDoS) attack, saturating both the inter-satellite links (ISLs) and the satellite-to-ground station communication channels.

(G. Giuliani et al. "ICARUS: Attacking Low Earth Orbit Satellite Networks". In: *2021 USENIX Annual Technical Conference (USENIX ATC 21)*. USENIX Association, 2021, pp. 317–331)

Take control of a satellite via remote exploit

LEO (Low Earth Orbit)

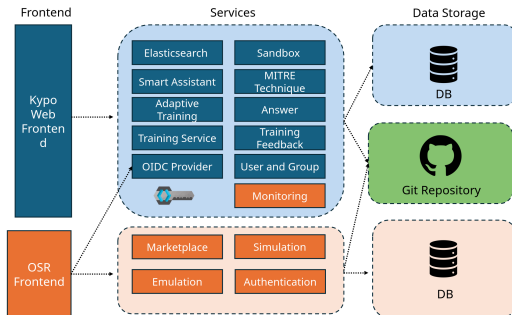


Scenario³:

- The student obtains a copy of the satellite's firmware.¹
- Through reverse engineering, they discover a buffer overflow vulnerability.
- They develop an exploit script that causes the satellite to behave abnormally - for example, by altering a wather satellite to broadcast custom data such as a Bitcoin ransom message.

(J. Willbold et al. "Space Odyssey: An Experimental Software Security Analysis of Satellites". In: *2023 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, 2023, pp. 1–19. DOI: 10.1109/SP46215.2023.10351029)

OSR Architecture



Conclusions

- Security by obscurity is generally recognized as a poor security practice, and this principle equally applies to the domain of satellite cybersecurity.
 - There is a clear need for dedicated tools and frameworks to test satellite infrastructures and conduct practical training exercises.
- OpenSatRange addresses this gap by providing an efficient and reliable cyber range platform that enables comprehensive testing and evaluation of satellite systems.
- Its modular architecture supports the design and implementation of diverse training scenarios, covering a wide range of aspects within satellite cybersecurity.

Thanks for the attention!

Bibliography I

- [1] Gregory Falco. “The vacuum of space cyber security”. In: *2018 AIAA SPACE and Astronautics Forum and Exposition*. Reston, Virginia: American Institute of Aeronautics and Astronautics, Sept. 2018.
- [2] G. Giuliari et al. “ICARUS: Attacking Low Earth Orbit Satellite Networks”. In: *2021 USENIX Annual Technical Conference (USENIX ATC 21)*. USENIX Association, 2021, pp. 317–331.
- [3] J. Willbold et al. “Space Odyssey: An Experimental Software Security Analysis of Satellites”. In: *2023 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, 2023, pp. 1–19. DOI: [10.1109/SP46215.2023.10351029](https://doi.org/10.1109/SP46215.2023.10351029).