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

[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

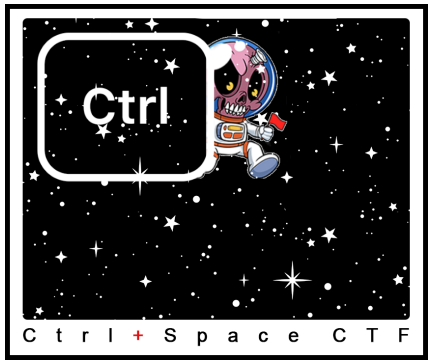
AWS Ground Station

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

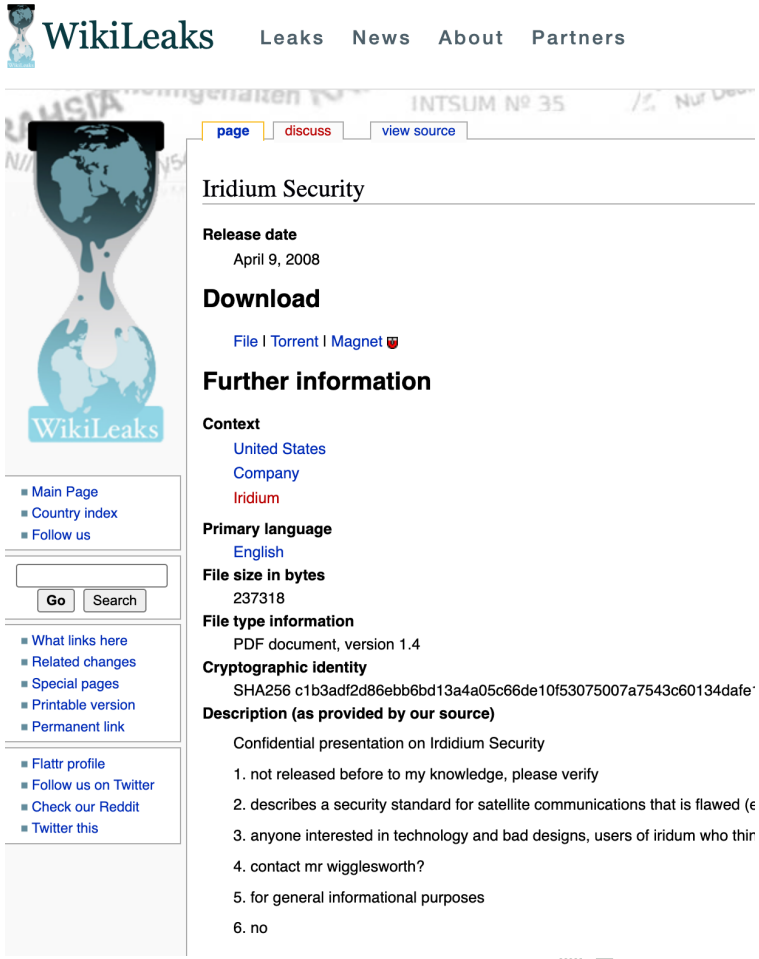
Get started with AWS Ground Station

GaaS

SDR



CTF

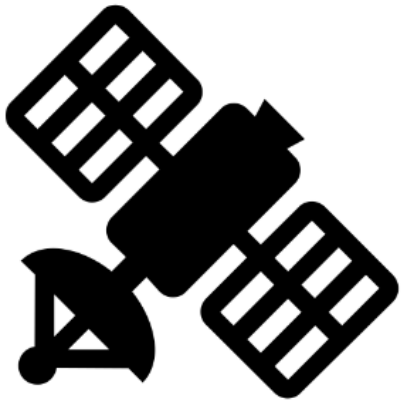


Levels of Enlightenment in Satellite Cybersecurity

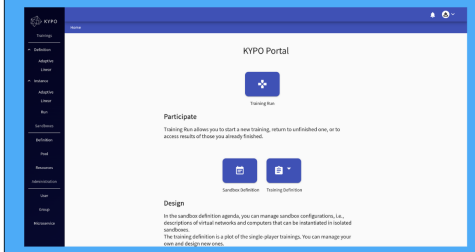
Filling the vacuum: OpenSatRange

- CyberRange for Satellite Systems

+



Kypo



Intuitive Graphic Interface

User Activity Monitoring System

KYPO

Cyber Range Platform

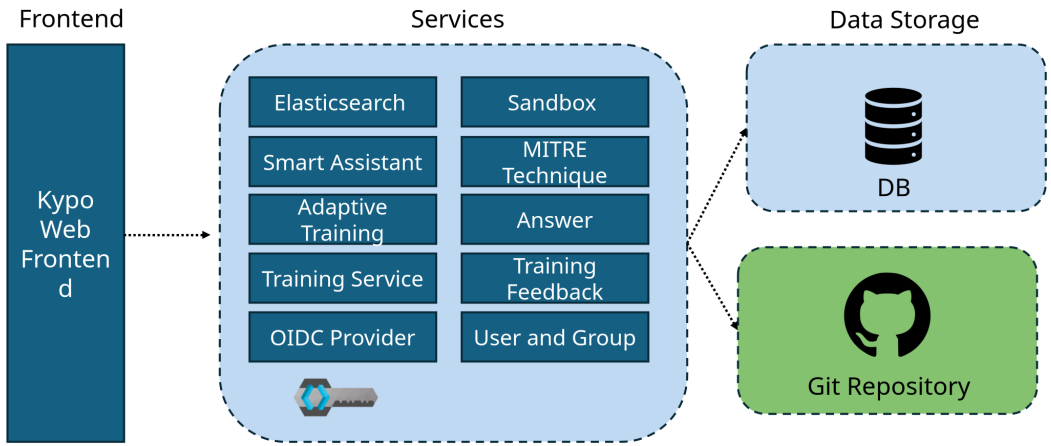
KEYCLOAK

Keycloak Integration

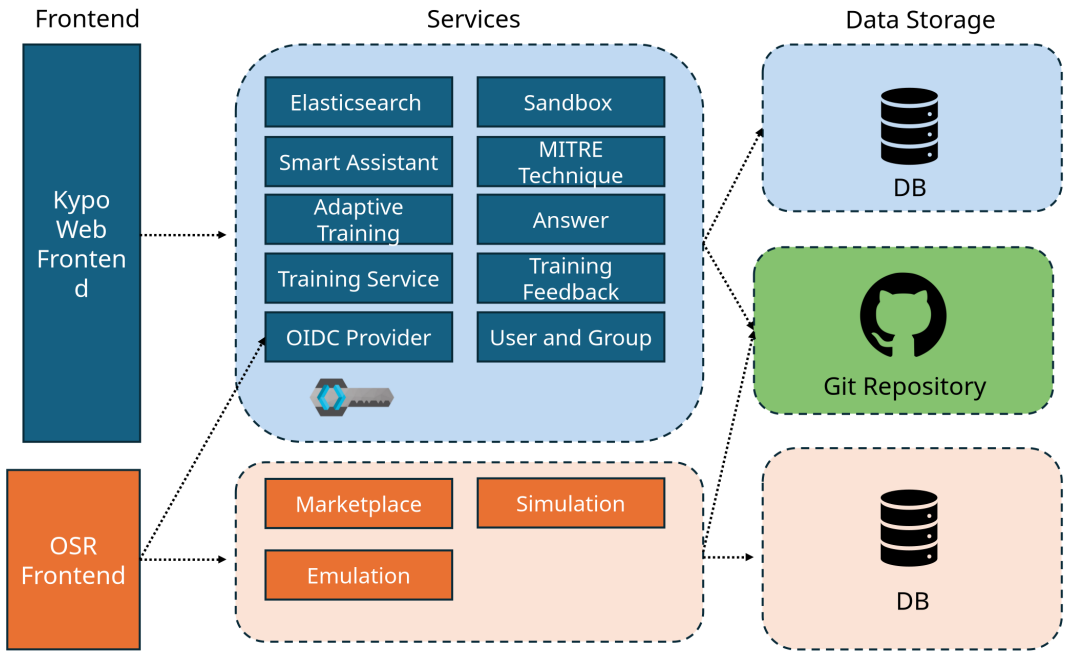
Git & Github

Git Repository for Sandbox Management

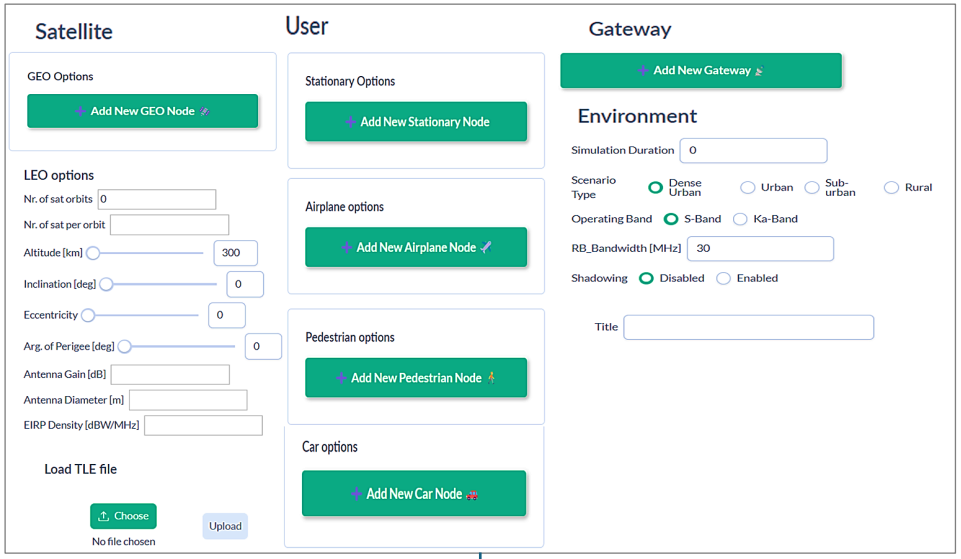
OSR Architecture

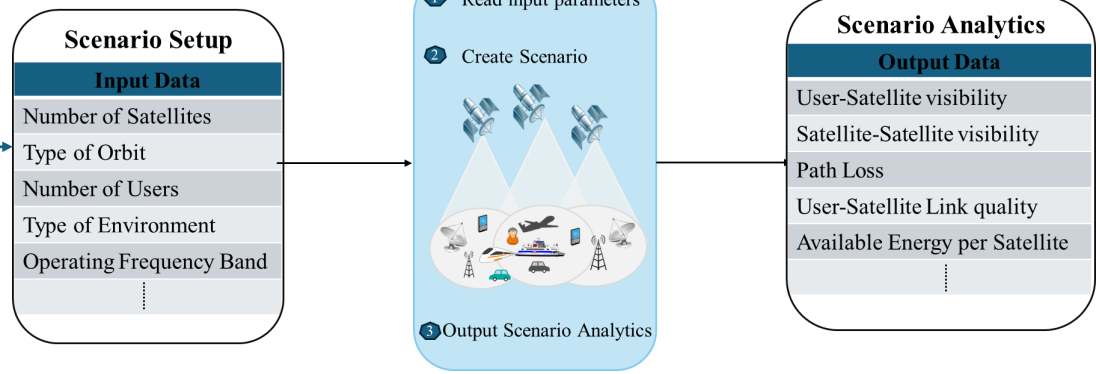


OSR Architecture



Satellite Simulation





SIMULATION → EMULATION → MARKETPLACE

Satellite Simulation

Different Mobility Models and Coordinate Systems

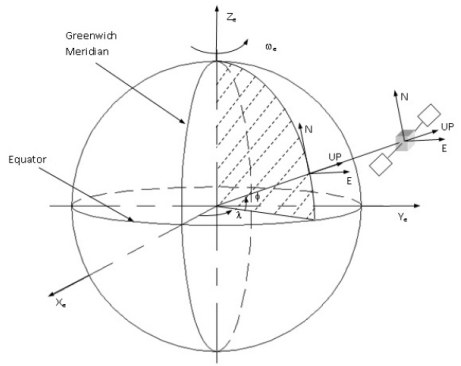
Higher Distance-Higher Delays

Different Antenna Models

Different Channel Model

ns-3 Network Simulator

Figure. 2 ECEF and navigation frames.



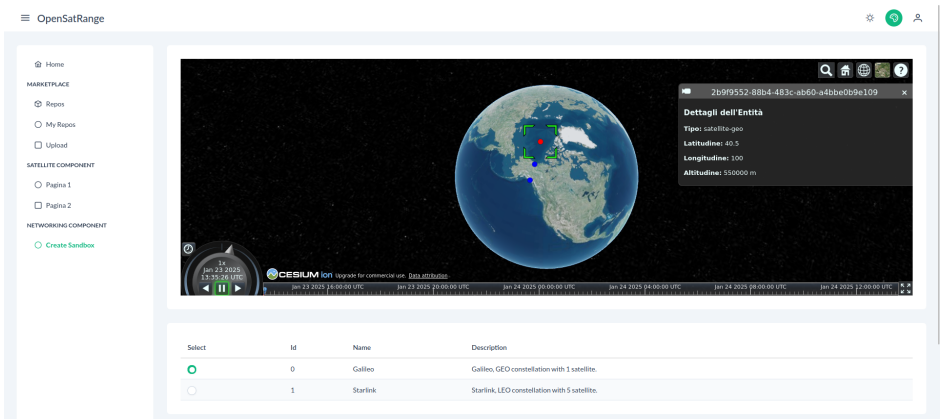
Elevation	S-band			Ka-band		
	LOS	NLOS		LOS	NLOS	
	σ_{SF} (dB)	σ_{SF} (dB)	CL (dB)	σ_{SF} (dB)	σ_{SF} (dB)	CL (dB)
10°	3.5	15.5	34.3	2.9	17.1	44.3
20°	3.4	13.9	30.9	2.4	17.1	39.9
30°	2.9	12.4	29.0	2.7	15.6	37.5
40°	3.0	11.7	27.7	2.4	14.6	35.8
50°	3.1	10.6	26.8	2.4	14.2	34.6
60°	2.7	10.5	26.2	2.7	12.6	33.8
70°	2.5	10.1	25.8	2.6	12.1	33.3
80°	2.3	9.2	25.5	2.8	12.3	33.0
90°	1.2	9.2	25.5	0.6	12.3	32.9

SIMULATION → EMULATION → MARKETPLACE

cnit Agenzia Spaziale Italiana

Satellite Emulation

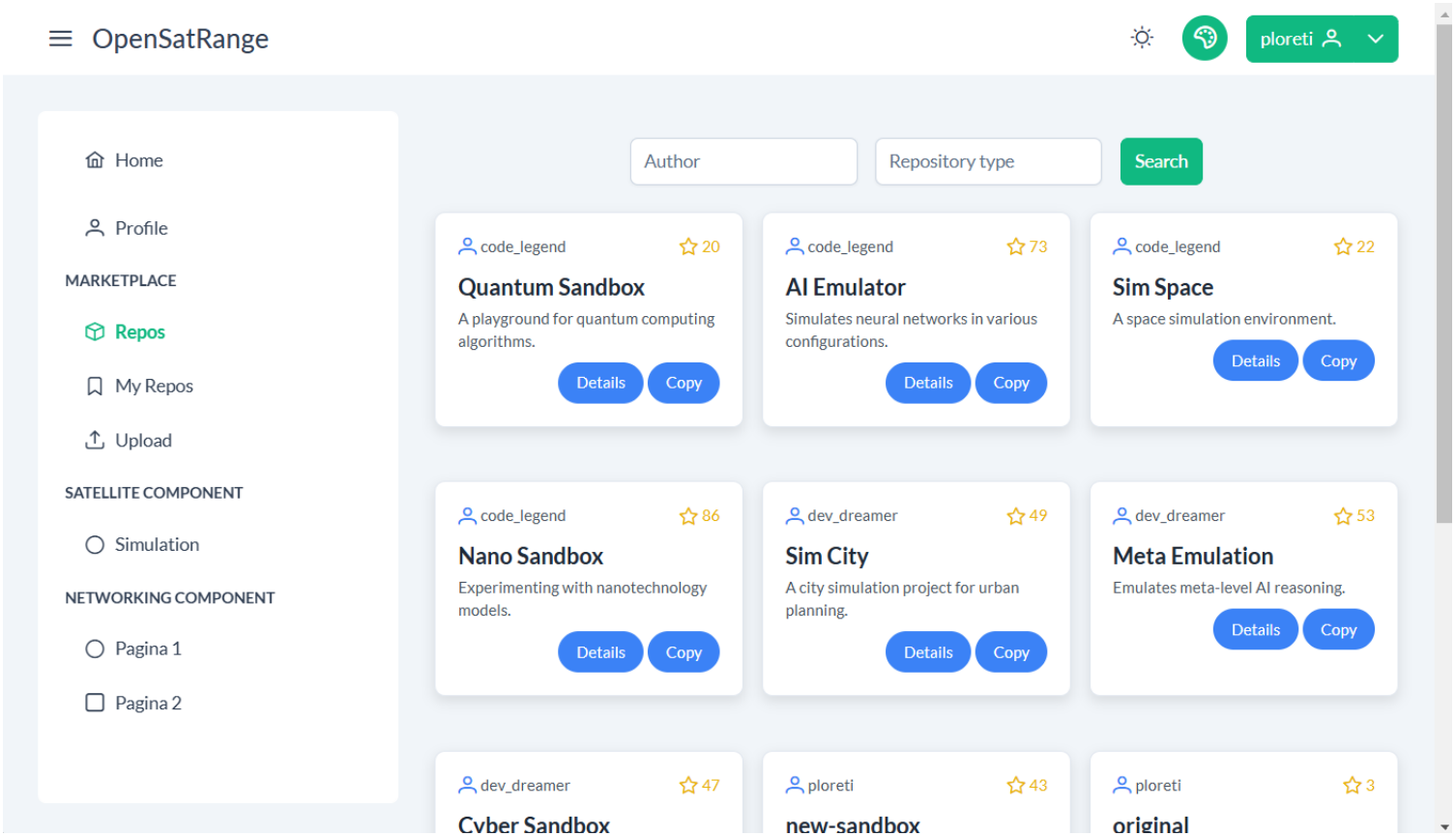
- GEO:
  - Each network segment is modeled as an OpenStack virtual network;
  - Each entity is represented by a dedicated virtual machine with an OpenSAND.



- 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.

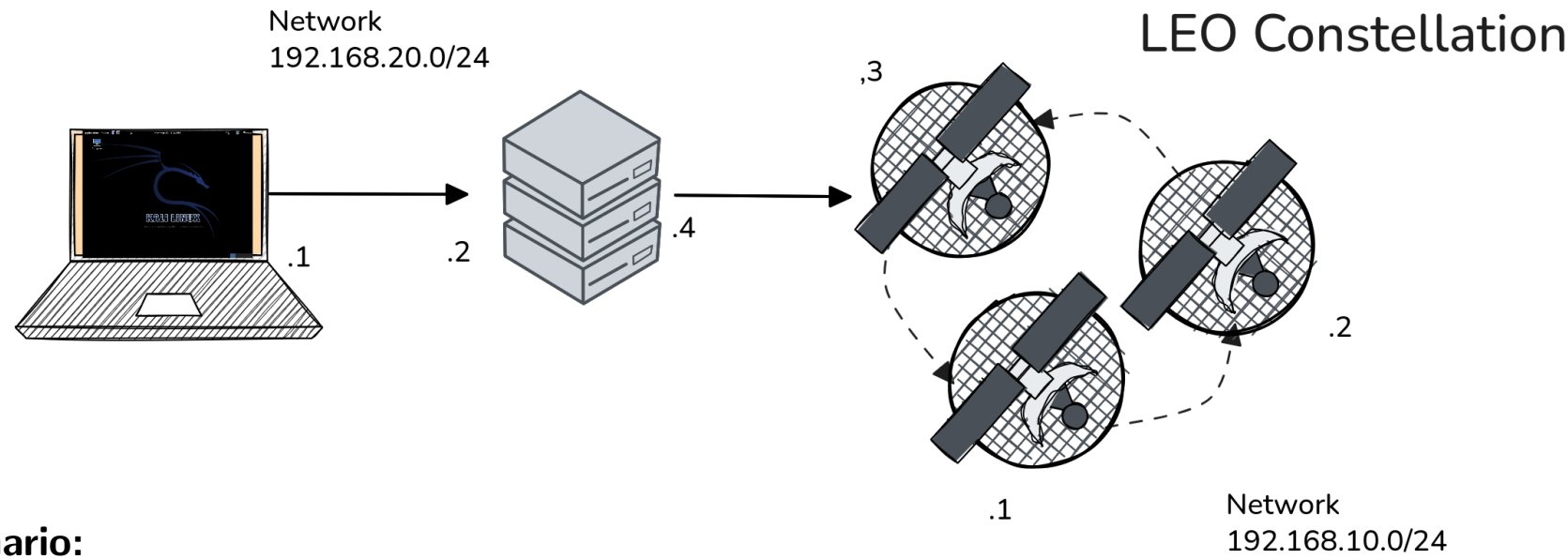
SIMULATION --- EMULATION --- MARKETPLACE

Marketplace



Tampering with the firmware of a satellite

LEO (Low Earth Orbit)

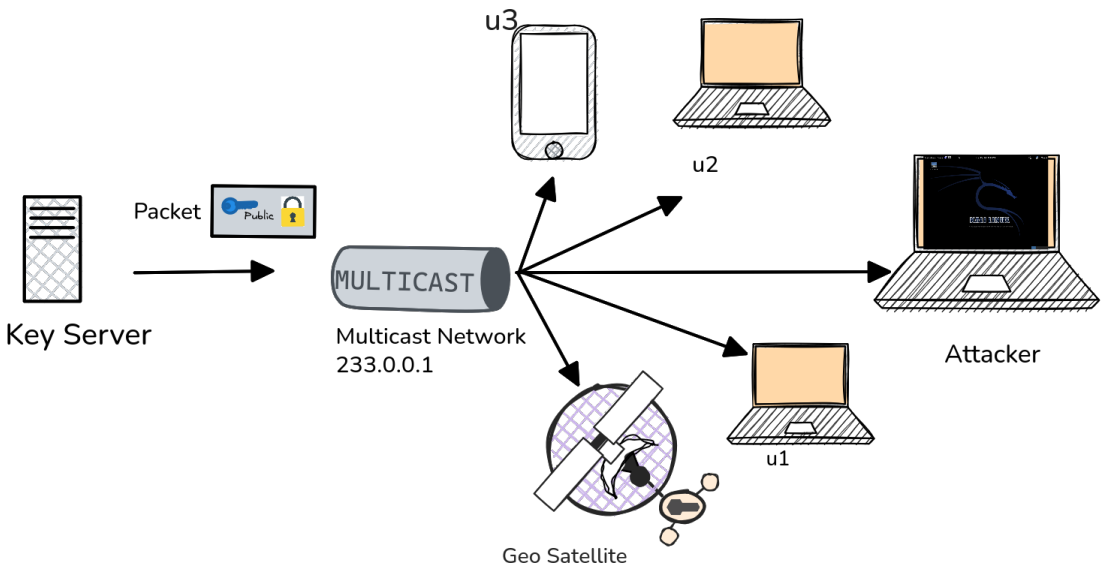


Scenario:

- 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 the 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)

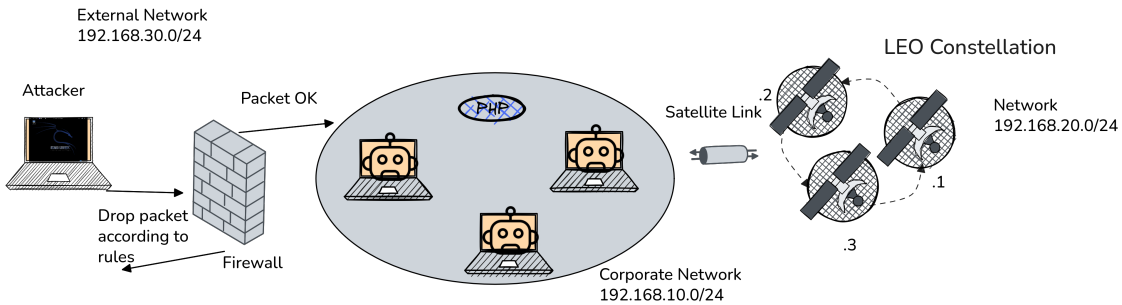


Scenario:

- 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)



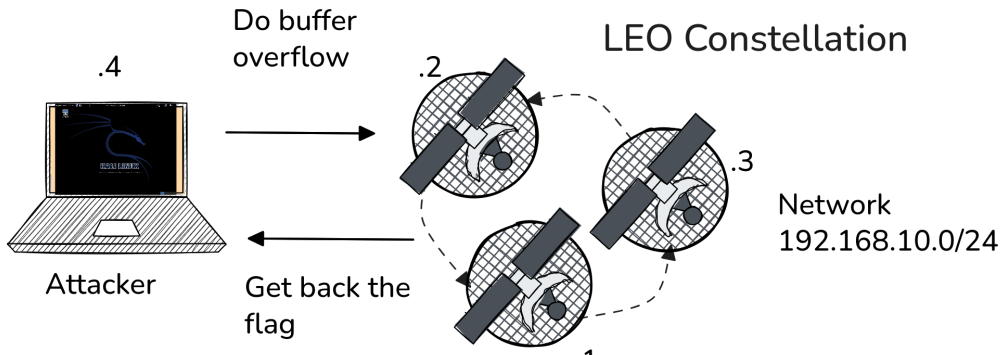
Scenario[2]**:**

- 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. 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)

Take control of a satellite via remote exploit

LEO (Low Earth Orbit)

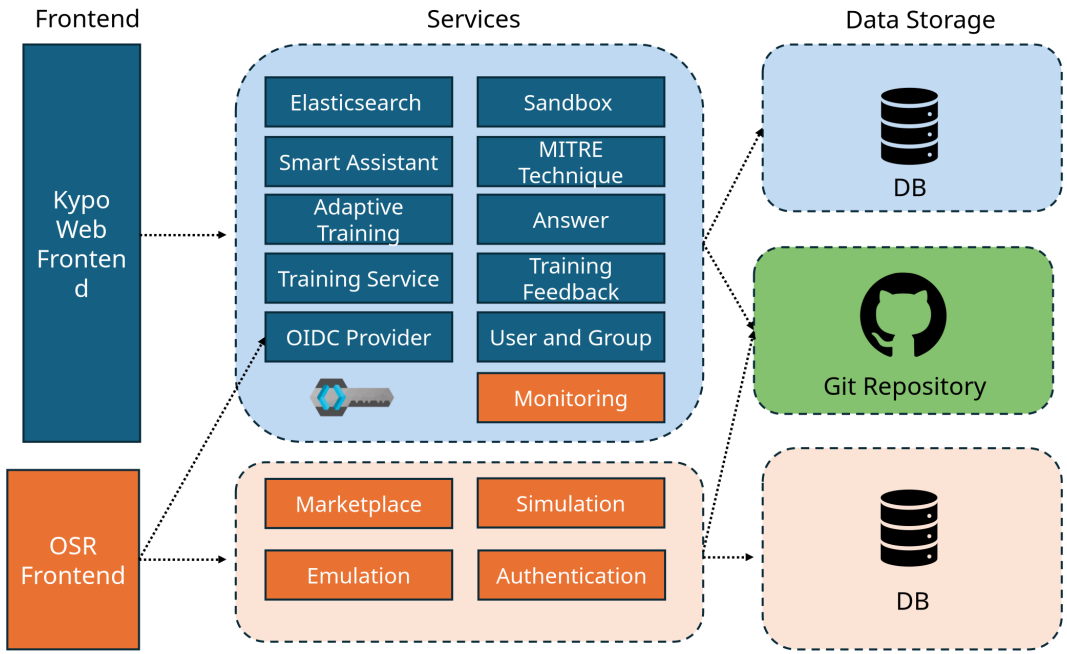


Scenario[3]**:**

- The student obtains a copy of the satellite's firmware.
- 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.