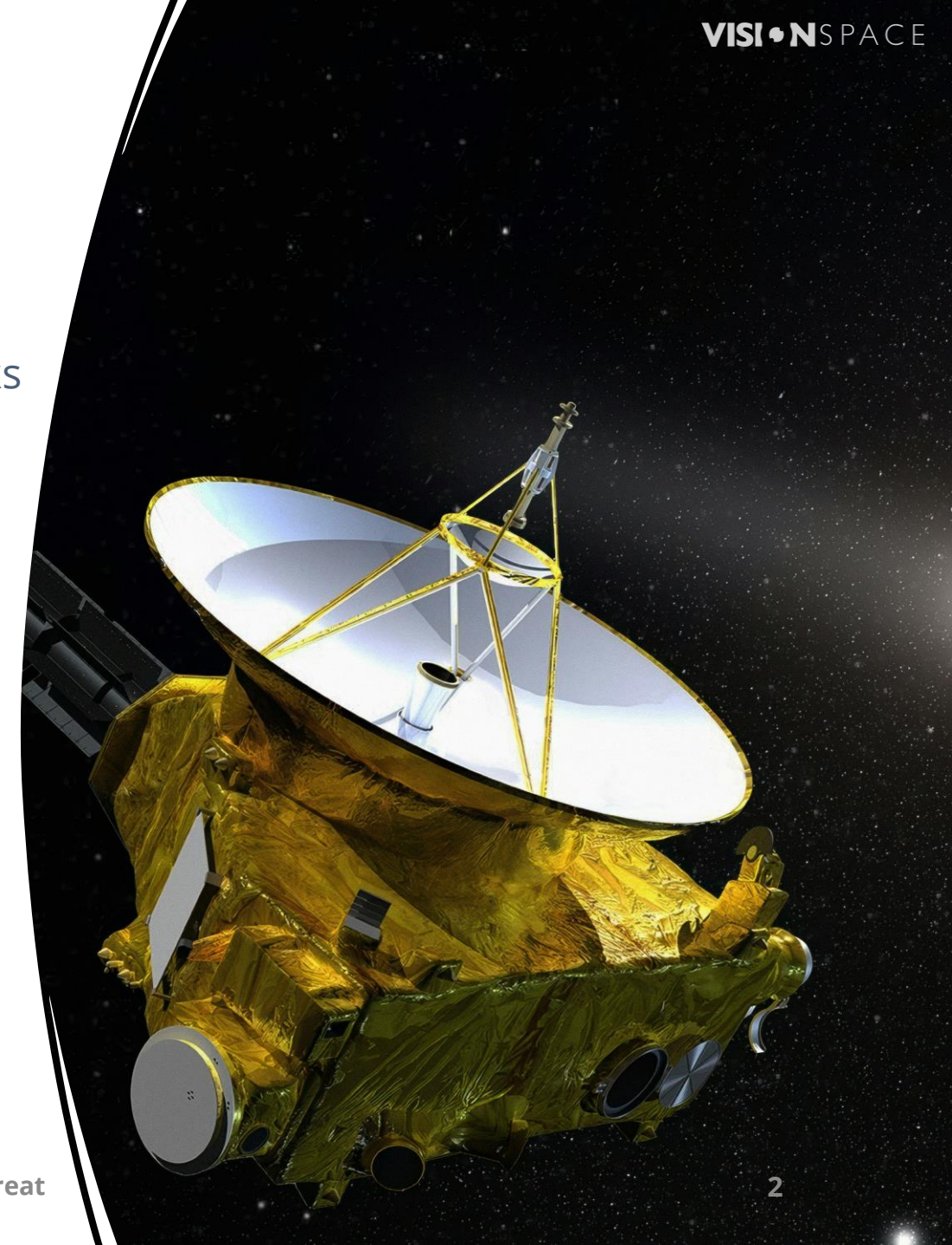
Ground Control to Major Threat

VISION SPACE

Hacking the Space Link Extension Protocol

Introduction

- **space missions,** increasingly the subject of cyber attacks
- **space vs ground,** as the attack surface
- **SLE protocol**, as the main communication standard
- **SLE security** and its known vulnerabilities
- **exploitation** methods and techniques
- possible **mitigations** and the future of SLE



Space and Ground

Space Segment

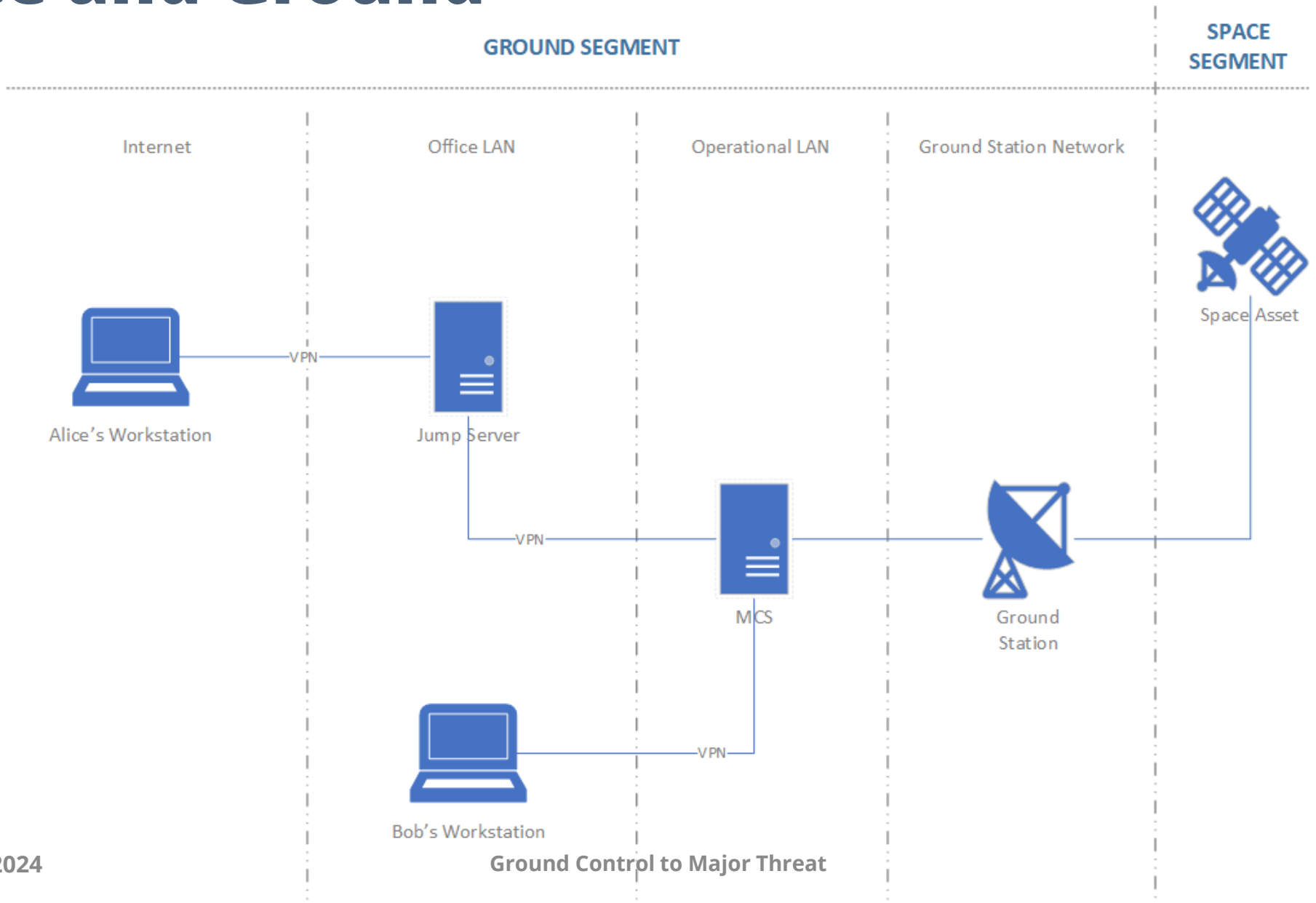
- very complex
- single entry point/interface – small attack surface
- challenging communication (visibility, orbit, distance)

Ground Segment (+ user segment)

- many interconnected components - large attack surface
- many potential points of vulnerability
- no sophisticated equipment is required



Space and Ground



Space and Ground



SLE Role

SLE Protocol One (ISP1)

- forward space link data units
- return space link data units
- based on TCP/IP
- supports transport, encoding and authentication
- doesn’t specify methods or technologies for communication
- SLE Provider (e.g. ground station)
- SLE User (e.g. Mission Control System)



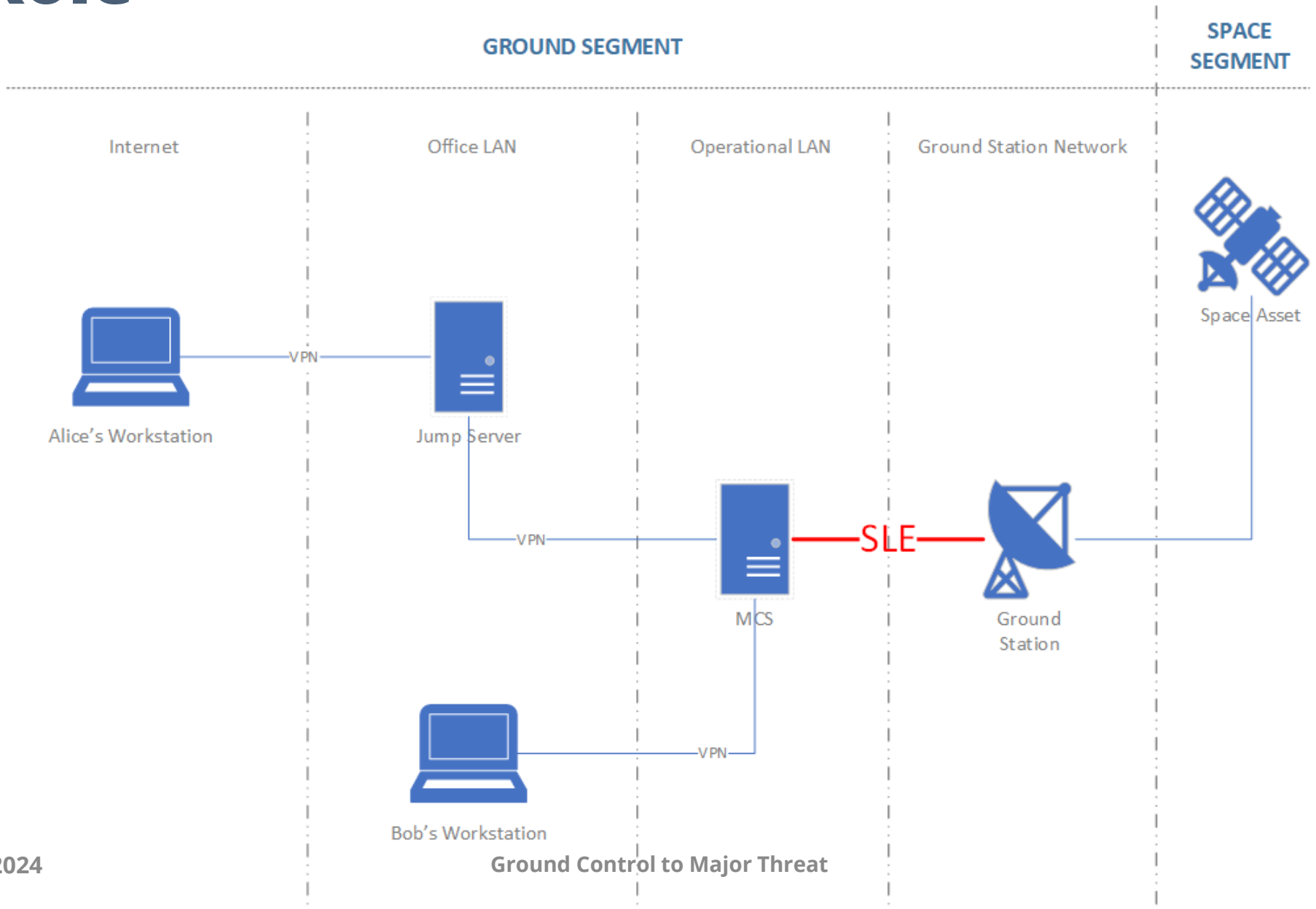


SLE Role

SLE in a nutshell

Defines a protocol for transferring SLE Protocol Data Units (PDUs) using TCP/IP for data transfer, and Abstract Syntax Notation One (ASN.1) for data encoding.

SLE Role


GROUND SEGMENT
SPACE SEGMENT
Internet
Office LAN
Operational LAN
Ground Station Network
Space Asset
VPN
Alice's Workstation
Jump Server
VPN
MCS
SLE
Ground Station
VPN
Bob's Workstation

Real-world Applications







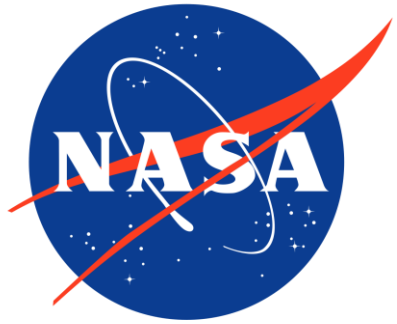
























Real-world Applications



RECOMMENDED STANDARD FOR SLE FCLTU SERVICE

At time of publication, the active Member and Observer Agencies of the CCSDS were:

Member Agencies

- Agenzia Spaziale Italiana (ASI)/Italy.
- Canadian Space Agency (CSA)/Canada.
- Centre National d'Etudes Spatiales (CNES)/France.
- China National Space Administration (CNSA)/People's Republic of China.
- Deutsches Zentrum für Luft- und Raumfahrt (DLR)/Germany.
- European Space Agency (ESA)/Europe.
- Federal Space Agency (FSA)/Russian Federation.
- Instituto Nacional de Pesquisas Espaciais (INPE)/Brazil.
- Japan Aerospace Exploration Agency (JAXA)/Japan.
- National Aeronautics and Space Administration (NASA)/USA.
- UK Space Agency/United Kingdom.

Real-world Applications

CORTEX Products

	CORTEX CRT TT&C Modem	CORTEX HDR High Rate Payload Demodulator
	The Universal TT&C Modem, World Reference for Securing Operations for the past 20 years	The Most Powerful and Flexible High Data Rate Demodulator for Earth Observation Payload
	Narrowband Communications in S-Band, L-Band, X-Band	Wideband Communications in X-Band and Ka-Band
Key Features	Doppler Compensation Diversity combining Pre-D and Post-D Spread Spectrum Real Time Automatic Equalizer - DEAF	Real Time Automatic Equalizer - DEAF Cross-Polarization Cancellation - XDEAF Diversity Combining
Downlink	Up to 40 Mbps, 6 Channels, 3 Inputs	Up to 10 Gbps, 6 Channels, 2 Inputs
Ranging	Active, Semi Active, Hybrid	-
Telecommand	Up to 1 Mbps, 2 Outputs	-
Test Modulator	Noise Generation Data Playback	Dual IF-out, Noise, Doppler & XFD Generation Group Delay Simulation Data Playback
Interfaces	[illegible]	720 MHz, 12 GHz, 2.4 GHz 2 Inputs for Dual Polarization Transmissions
	[illegible]	2 x 1 GigE, 2 x 10 GigE
	Multiple Te[illegible]	A.I.T. Interface: EC1, LVDS/WizardInk
Data Recording and Processing	RAW, CADU, Up to 500 GB Storage	RAW, CADU, VCDU, APID Up to 12 TB Storage
Miscellaneous	SLE, COP-1, STI 100113	SLE, STI 100113

	CORTEX RSR Record and Replay	CORTEX WBR Record and Replay
Record & Replay Aggregate Bandwidth	Up to 160 MHz	
Interfaces	70 MHz, L-Band, S-Band	720 MHz, 12 [illegible]
	2 x 1 GigE	2 x 1 GigE, 2 x [illegible]
Quality of Signal	Degradation <0.5 dB	Group Delay Variation [illegible]
Recording Time at Full Rate	Up to 5h	Up to 5h

	Converters		
	S-Band	X-Band	Ka-Band
Models	Up and Down	Up and Down	Up and Down
RF Interface	Up: 2025 - 2120 MHz Down: 2200 - 2300 MHz	7900 - 8500 MHz	25.5 - 27.0 GHz
IF Interface	70 MHz	720 MHz	1200 MHz 1500 MHz 2400 MHz
Impedance	50 Ohms	50 Ohms	50 Ohms
VSWR	< 1.3	< 1.4	< 1.5

Ground Station Specifications

	MODEL	LEGION 400	VISION 610 / 720	ORION 720	ORION 930	ORION 1100	ORION 1300
	DIAMETER	3,9 m	5,5 m	7,3 m	9,3 m	11,5 m	13,5 m
	CONFIGURATION	Mono, Bi or Tri-Band X or S+X or S+Ka or S+X+Ka					
X-Band RX (7,900 - 8,500 GHz)	G/T Mid-Band, 5° Elevation, Clear Sky, +20°C, Continental tri board	26,5 dB/K	>30,5 dB/K	>33 dB/K	>34,5 dB/K	>36,5 dB/K	>36,5 dB/K
	Rx Polarization	LHCP and RHCP (simultaneous)					
	Specific Filtering	Included - Radar Low Pass Filter or Band Pass Filter					
S-Band RX (2,200 - 2,300 GHz) TX (2,025 - 2120 GHz)	G/T Mid-Band, 5° Elevation, Clear Sky, +20°C, Continental	>13,5 dB/K	>17 dB/K	>19,5 dB/K	>21,5 dB/K	>23,5 dB/K	>25 dB/K
	Rx Polarization	LHCP and RHCP (simultaneous)					
	ERP @Peak Baseline	45 dBW	56 dBW	58 dBW	60 dBW	61,5 dBW	62,5 dBW
	Tx Polarization	LHCP or RHCP (switchable)					
Ka-Band RX (25,500 - 27,000 GHz)	G/T Mid-Band, 5° Elevation, Clear Sky, +20°C, Continental	>31,5 dB/K	>35 dB/K	>37,5 dB/K	>39,5 dB/K	>41,5 dB/K	>43 dB/K
	Rx Polarization	LHCP and RHCP (simultaneous)					
Mode of Operations	Auto-Track Mode	Single Channel Monopulse - Triband/Polarization switchable in each band (SAFRAN patented)					
Accuracies	Tracking Accuracy	0,03°rms	0,05°rms	0,02°rms	0,02°rms	0,02°rms	0,02°rms
	Pointing Accuracy	0,04°rms	0,05°rms	0,04°rms	0,04°rms	0,04°rms	0,04°rms
Environmental Conditions	Operating Wind S/X-Band	90 km/h gust	90 km/h gust	110 km/h gust	90 km/h gust	90 km/h gust	90 km/h gust
	Operating Wind Ka-Band	90 km/h gust	90 km/h gust	90 km/h gust	90 km/h gust	90 km/h gust	90 km/h gust
	Operating Temperature	-20°C to +50°C -40°C to +50°C with available options: winter package, deicing, radome					



Converters



CORTEX DTR



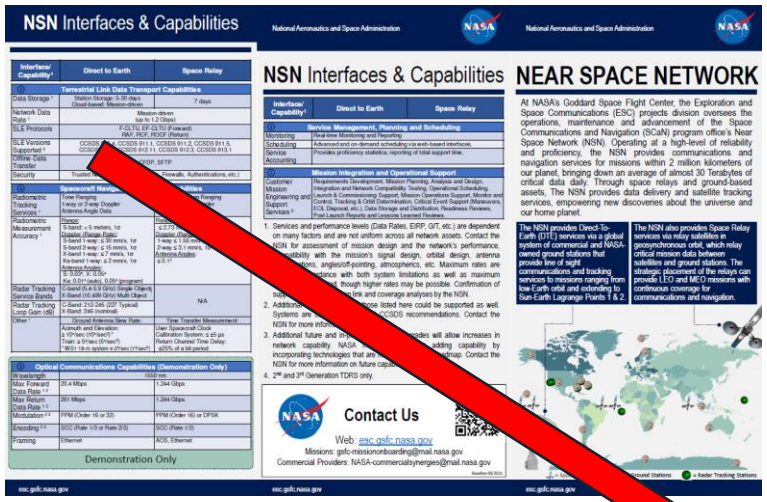
CORTEX HDR



CORTEX CRT

Miscellaneous	SLE, COP-1, STI 100113	SLE, STI 100113

Real-world Applications



NSN Interfaces & Capabilities

Interface/ Capability[1]	Direct to Earth	Space Relay
③ **Terrestrial Link Data Transport Capabilities**		
Data Storage [1]	Station Storage: 5-30 days Cloud-based: Mission-driven	7 days
Network Data Rate [1]	Mission-driven (up to 1.2 Gbps)	
SLE Protocols	F-CLTU, EF-CLTU (Forward) RAF, RCF, ROCF (Return)	
SLE Versions Supported [2]	CCSDS 910.4, CCSDS 911.1, CCSDS 911.2, CCSDS 911.5, CCSDS 912.1, CCSDS 912.11, CCSDS 912.3, CCSDS 913.1	
Offline-Data Transfer	CFDP, SFTP	
Security	Trusted Networks (Access Controls, Firewalls, Authentications, etc.)	
④ **Spacecraft Navigation Tracking Capabilities**		
Radiometric	Tone Ranging	Spread Spectrum Ranging

SLE FCLTU – Overview

FCLTU – Forward Communication Link Transmission Unit

- service that allows CLTU transmission to a spacecraft

Selected operations:

- CLTU-BIND (establish an association)
- CLTU-UNBIND (release an association)
- CLTU-START (prepare to receive)
- CLTU-STOP (stop production)
- CLTU-TRANSFER-DATA (transfer CLTUs)



SLE FCLTU – Security

Data Privacy (Confidentiality)
- doesn't exist

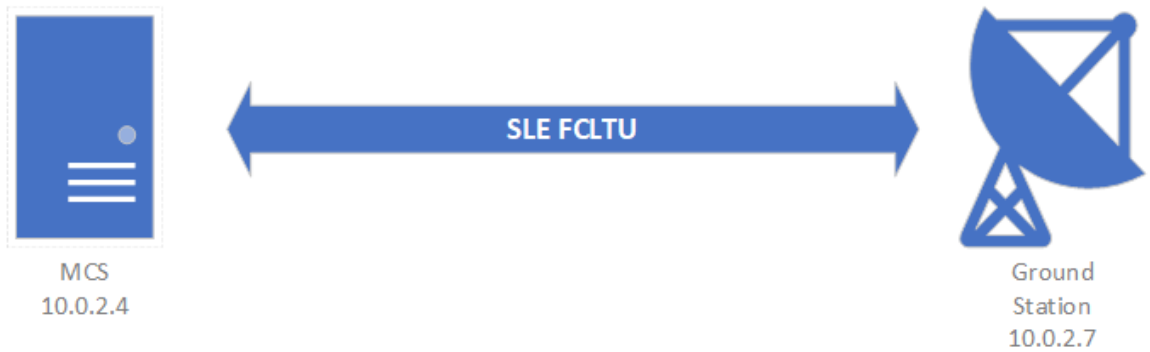
Data Integrity
- sequence numbers to prevent the op injection and seizing control (but not really)

Authentication
- vulnerable to MitM attacks



SLE FCLT – Testing Environment

GROUND SEGMENT (TEST ENVIRONMENT)



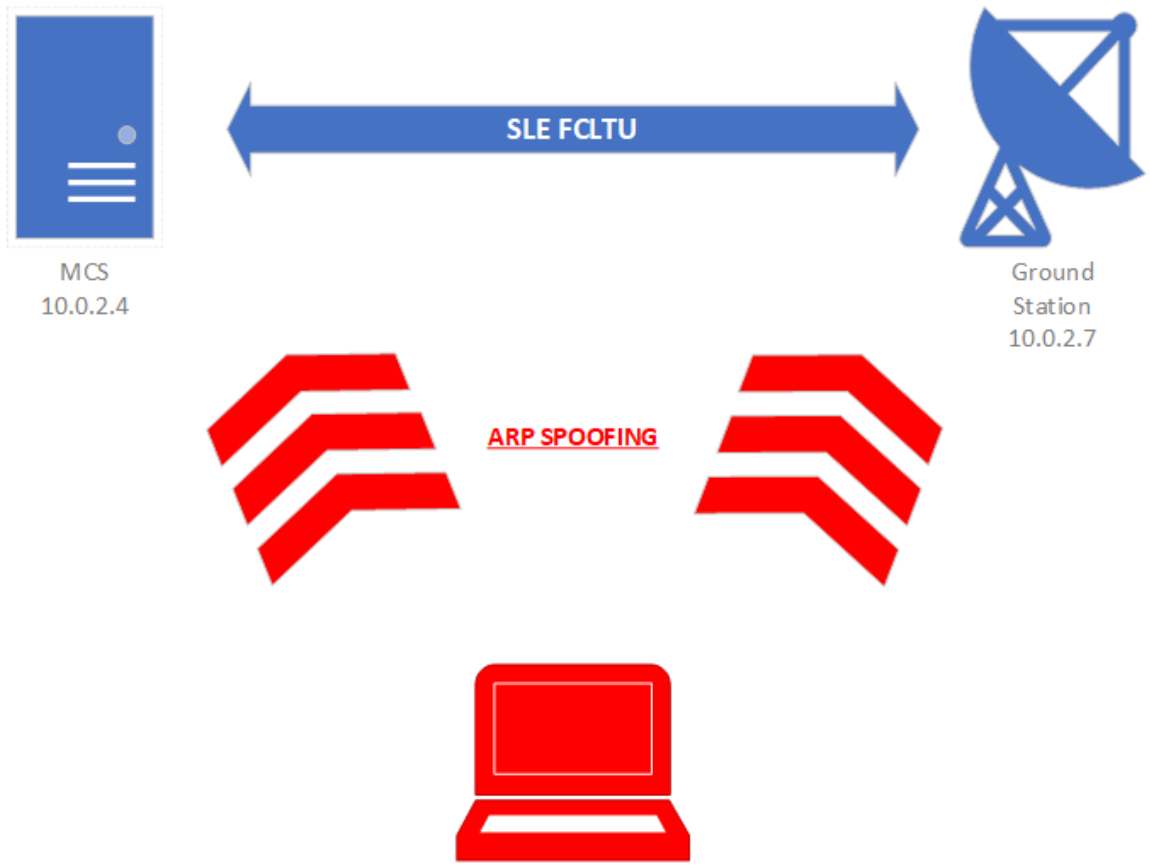
SLE Provider: plays the role of a ground station (GS), which runs Debian with the ESA SLE-API implementation

SLE User: plays the role of a Mission Control System (MCS), which runs Debian with the pythonsle Implementation

Attacker: a Kali host from which the attack is conducted

SLE FCLT – Technique Overview

GROUND SEGMENT (TEST ENVIRONMENT)

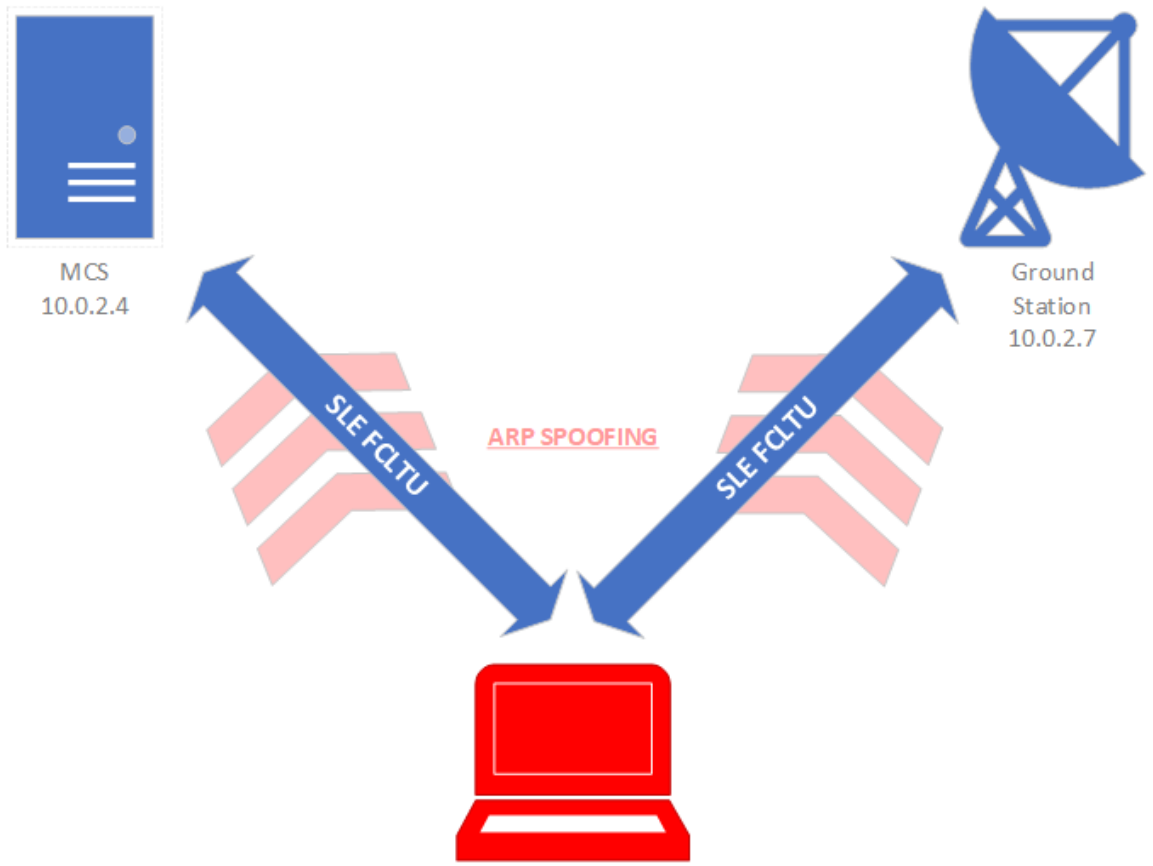


No encryption: vulnerable to MitM attack

- ARP spoofing
- capture at the TCP frame level
- decode ISP1 frames
- manipulate the content of CLTU
- update and forward the TCP frame

Exploitation – ARP spoofing

GROUND SEGMENT (TEST ENVIRONMENT)



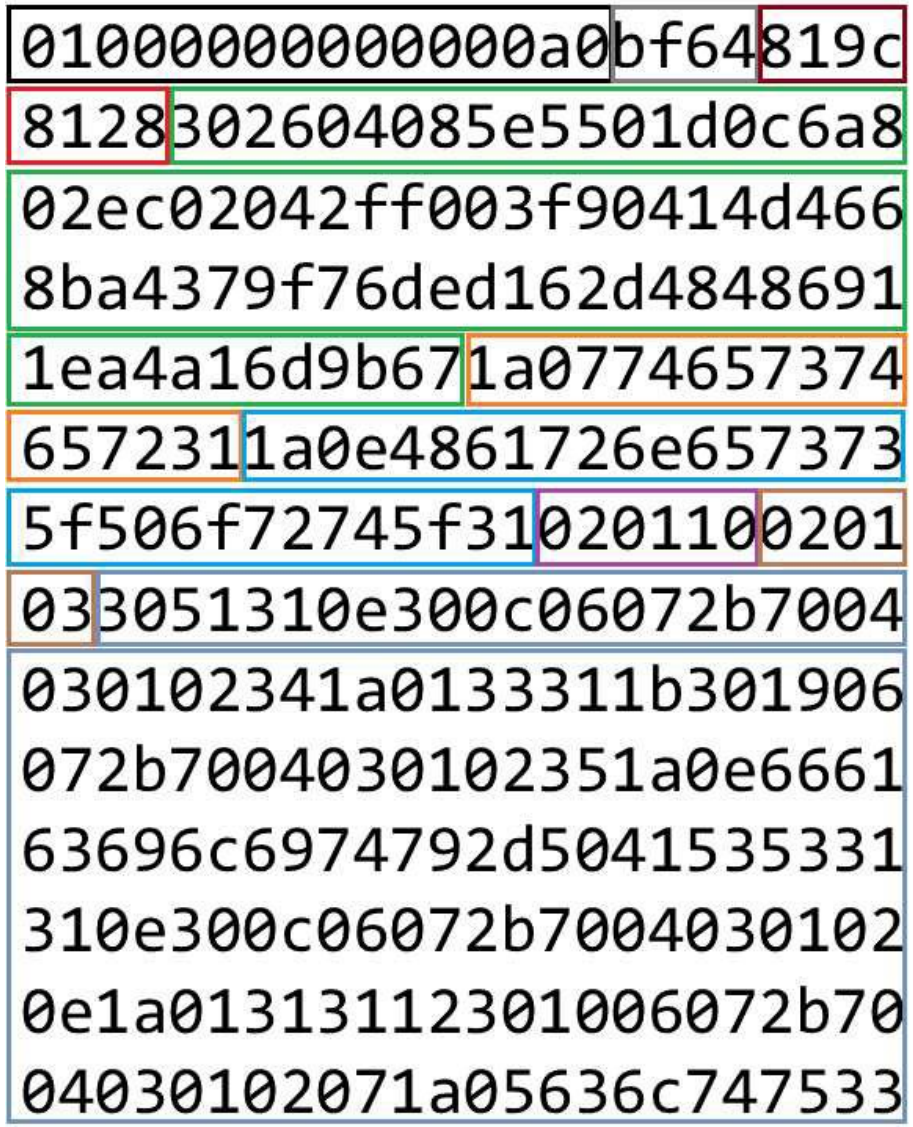
- poison ARP tables of MCS and Ground Station hosts
- make the traffic go through the attacker's host
- capture the TCP frames in the *netfilter_queue* for processing

Exploitation
- Processing CLTU Frames

- TCP Frame data field contains SLE PDUs in the ISP1 format
- ISP1 uses ASN.1 encoding to transfer the SLE PDUs, which must be decoded following the ASN.1 TLV (Tag-Length-Value) of BER (Basic Encoding Rules)for the privative data types, ISP1 uses the standard TLV
- besides standard TLV, ISP1 implements custom, context-specific structures
- for our exploitation demo, we focus only on the tags related to CLTU
- after decoding, the fields must be interpreted using the FCLTU Data Type Specification



Exploitation – Example of Decoding



ISP1 Header

Main structure (class and length)

CLTU Bind message structure (class and length)

CLTU Bind invoker-credentials structure (class and length)

CLTU Bind invoker-credentials

CLTU Bind - service-instance-identifier

CLTU Bind responder-port-identified

CLTU Bind service-type

CLTU Bind version number

CLTU Bind service-instance-identifier

Demo - Nominal Behavior

- establishing the connection by transmitting the CLTU-BIND
- initiating the Service Instance via the transmission of CLTU-START
- sending the data using CLTU-TRANSFER_DATA
- halting the Service Instance by dispatching CLTU-STOP
- closing the connection by issuing the CLTU-UNBIND



Demo: SLE Provider - User exchange - EDIT.mp4

Demo - Preventing FCLTU BIND

- capture TCP frame exchanges between the SLE User and the SLE Provider
- processing of the Data Field within the TCP Frame
- validation to determine if the TCP Frame includes user BIND credentials
- modification of specific bytes within the credentials structure, if found



Demo: SLEuth - Prevent Auth - EDIT.mp4

Demo – Capture Credentials

- capture the TCP frame exchanges between the SLE User and the SLE Provider
- process the Data Field of the TCP Frame
- check whether the TCP Frame contains user BIND credentials
- capture and display/store the credentials



Demo: SLEuth - Capture Credentials - EDIT.mp4

Demo – Tampering the Data

- capture the TCP Frame containing the CLTU-TRANSFER_DATA PDU, which includes the telecommanding products destined for the spacecraft
- update the content of the TCP Frame with the desired telecommanding data
- forward the updated TCP Frame to the receiving end



Demo: SLEuth - Tampering the Data - EDIT.mp4

Demo – Taking Over the SLE Session

- capture the BIND and manipulate the credential structure bytes to hinder successful authentication

- the attacker reuses the captured credentials and sends their own crafted BIND message to the SLE Provider, establishing a session between the Attacker and the SLE Provider

- with the successful session establishment, the attacker can command both the SLE Provider and the spacecraft for the duration defined in the AUTHENTICATION_DELAY configuration, leveraging the captured credentials



Demo: SLEuth - Taking over the SLE session - EDIT.mp4

Conclusions

- one of many methods to take over the control of spacecraft
- focused on commanding capabilities, but there's also telemetry
- knowledge of the spacecraft itself is required, but…
- all the knowledge can be gathered using OSINT
- ALL vs EVERY
- CCSDS SDLS (Space Data Link Security) for space only
- upcoming CCSDS PKI concepts could enable TLS-like features in ISP1



Future Work

- testing in ESA SMILE Lab
  - an actual ground station
  - includes CORTEX with an SLE service
- further development of SLEuth exploit
  - additional ways of exploiting the SLE
  - release as open-source



Resources

Full list in the publication

7 References

[1] Space Link Extension – Forward CLTU Service Specification, CCSDS 912.1-B-5, July 2023

[2] Space Link Extension – Internet Protocol for Transfer Services, CCSDS 913.1-B-2, September 2015

[3] Cross Support Transfer Service Specification Framework Concept, CCSDS 920.0-G-1, 2023

[4] Cross Support Transfer Service – Specification Framework, CCSDS 921.1-B-2

[5] Near Earth Network (NEN) Users' Guide, Goddard Space Flight Center, 2019

[6] Space Link Extension (SLE) Emulation for High-Throughput Network Communication, NASA Glenn Research Center

[7] CCSDS Recommended Procedures for Cloud-Based Interoperability Testing,

[8] DLR Portfolio – Ground Station Weilheim, accessed 2024-03-20

[9] Network Interface System, ESA's Next Generation CCSDS SLE Interface System, SpaceOps 2006

[10] Cortex SLE Provider System – From prototype to product, to successful operations. SpaceOps 2006

[11] Space Cybersecurity Lessons Learned from The ViaSat Cyberattack, 2022

[12] Near Space Network Brochure, accessed 2024-03-20

[13] Space Agencies, Ground Products and Solutions, SAFRAN, accessed 2024-03-20

[14] ASN.1 BER, accessed 2024-03-20

[15] ASN.1 Tags, accessed 2024-03-20

[16] Development of JAXA's SLE Gateway, SpaceOps 2004

[17] LibreCube SLE User Implementation in Python, GitHub, accessed 2024-03-20

[18] Viasat Hack, Wikipedia, accessed 2024-03-20

[19] Lessons Learned from the KA-SAT Cyberattack, Black Hat USA 2023, accessed 2024-03-20

[20] ESA SMILE Lab, ESA, accessed 2024-03-20

[21] ESA SLE-API, GitHub, accessed 2024-03-20

[22] ASN.1 JavaScript decoder (containing the SLE PDU), accessed 2024-03-20

[23] Safran CORTEX CRT, accessed 2024-04-02

[24] Space Data Link Security Protocol, CCSDS 355.0-B-2, July 2022



Further Research

- NASA OpenMCT part 1
- NASA OpenMCT part 2
- NASA AIT-Core
- YaMCS part 1
- YaMCS part 2



THANK YOU!

Andy Olchawa

andrzej.olchawa@visionspace.com

linkedin.com/in/andrzejolchawa

@0x4ndy

Milenko Starcik

milenko.starcik@visionspace.com

linkedin.com/in/milenko-starcik

