Covert Control: Unveiling Vulnerabilities
TT&C to Cyber Attack
CYSAT 202

Brandon Bailey, Randi Tinn
Cybersecurity and Advanced Platforms Subdivision (CA
Cyber Assessment & Research Dept (CA
The Aerospace Corporat

brandon.bailey@ae
240.521.4

Approved for Public Release via OTR-2024-00633

andon Bailey

Current Job: Principal Engineer, Cybersecurity and Advanced Platforms Subdivision (CAPS), at The Aerospace Corporation
- Developing cyber labs for training, perform penetration testing & vulnerability assessments {Ethical Hacking!}
- Performing cybersecurity research on ground systems and spacecraft systems to better position the federal government with respect to protection of our critical space infrastructure.

trical Engineering
ginia University

d Martin Supporting
Geospatial
ce Agency

2005 — LOCKHEED MARTIN

NASA's Independent Verification and Validation Program

Working for Small Business in West Virginia doing Spacecraft and Ground Simulation/Emulation

2009 — NASA

Transitioned to NASA Government Employee GS-13

Began "Hacking" Space Systems

2013 — NASA

Left the Government as GS-15 to become Chief Technology Officer (CTO) for small business in West Virginia

- Supported NASA part-time as contractor

2018

Left Job as CTO to join Aerospace Corporation Federally Funded and Development Center

2019 — AEROSPACE

2023

n-tested / "Ethically Hacked" Space Systems 2013-2024

Mars' Rovers (MER & MSL) & Deep Space Network (DSN) at JPL
Hubble Space Telescope (HST) at GSFC
Closed IONet (CIONet) within NASCOM at GSFC
Space Network (SN) at the White Sands Complex (WSC)
KSC Ground Systems Development and Operations (GSDO) Kennedy Ground Control System (KGCS) and Launch Control System (LCS)
James Web Space Telescope (JWST) Ground System at the Space Telescope Science Institute (STScI) in Baltimore
Huntsville Operations Support Center (HOSC) at Marshall Space Flight Center
Near Earth Network (NEN) at Wallops Flight Facility
ISS Mission Control Center (MCC) at Johnson Space Center
Wind tunnels at Glenn Research Center
Hypersonic Environment at Langley Research Center
NOAA's Joint Polar Satellite System (JPSS)

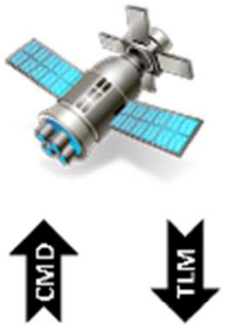
2019-2

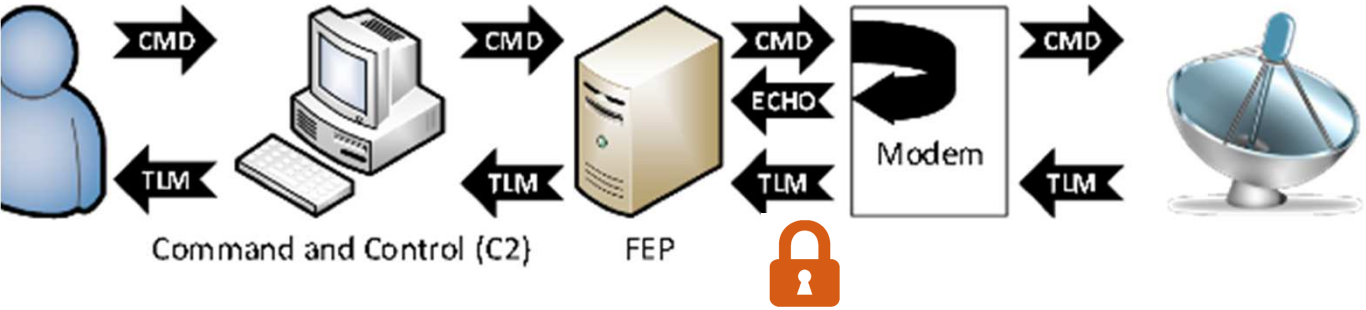
- DefCON Presentations:
  - DEF CON 2020: Exploiting Spacecraft
  - DEF CON 2021: Unboxing the Spacecraft Software BlackBox Hunting for Vulner
  - DEF CON 2022: Hunting for Spacecraft Zero Days using Digital Twins
  - DEF CON 2023: Building Space Attack Chains using SPARTA
- Papers/Articles:
  - 2019: Defending Spacecraft in the Cyber Domain
  - 2020: Establishing Space Cybersecurity Policy, Standards, & Risk Management
  - 2021: Cybersecurity Protections for Spacecraft: A Threat Based Approach
  - 2021: Translating Space Cybersecurity Policy into Actionable Guidance for Space V
  - 2022: Protecting Space Systems from Cyber Attack
- July 2022 Congressional Testimony:
  - Video: https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964
  - Written Testimony: https://republicans-science.house.gov/_cache/files/2/9/29 0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.202 bailey-testimony.pdf
- SPARTA Launched
  - https://sparta.aerospace.org

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

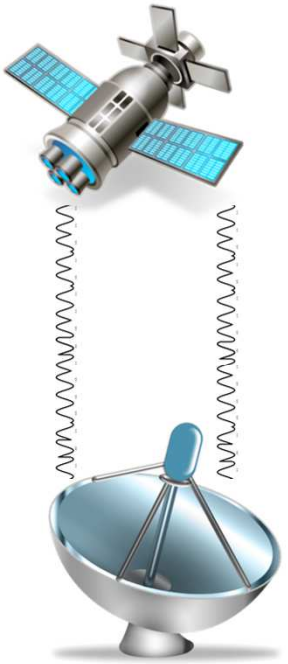
NASA's Exceptional Service Medal (2019) for "groundbreaking" cyber wo

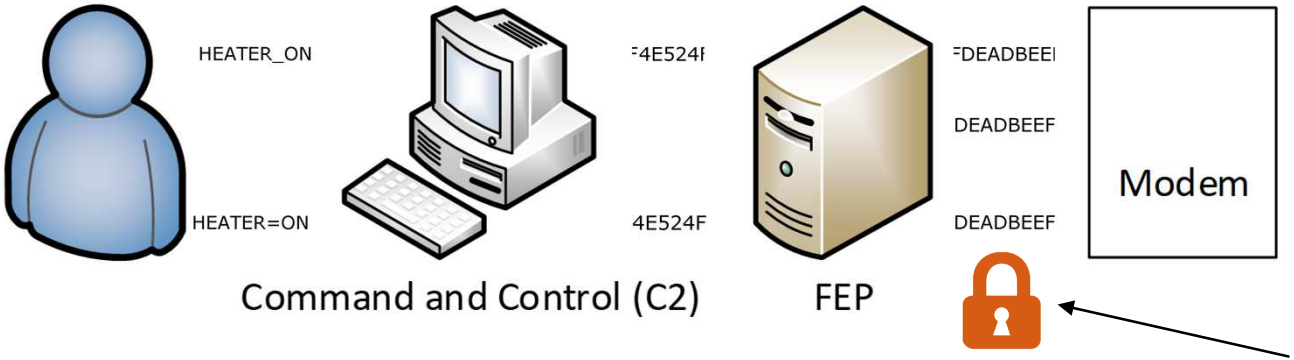
sics: Commanding & Telemetry





Bulk
Crypto Unit





Bulk
Crypto Unit

We got crypto…
we good right?

Not So
Fast My
Friend!!!

ılk Crypto Units (BCUs)

me Features … according to ChatGPT

Secure Communication Protocols

- *Implement secure communication protocols to establish encrypted channels between ground systems and spacecraft. These protocols ensure that data exchanged over the communication link is protected from interception, tampering, and unauthorized access.*

Encryption and Decryption

- *Encrypting and decrypting data transmitted between ground systems and spacecraft. They use cryptographic algorithms and keys to transform plaintext data into ciphertext before transmission and vice versa upon reception. Depending on BCU, full frame (including headers) or only payload frame.*

Key Management

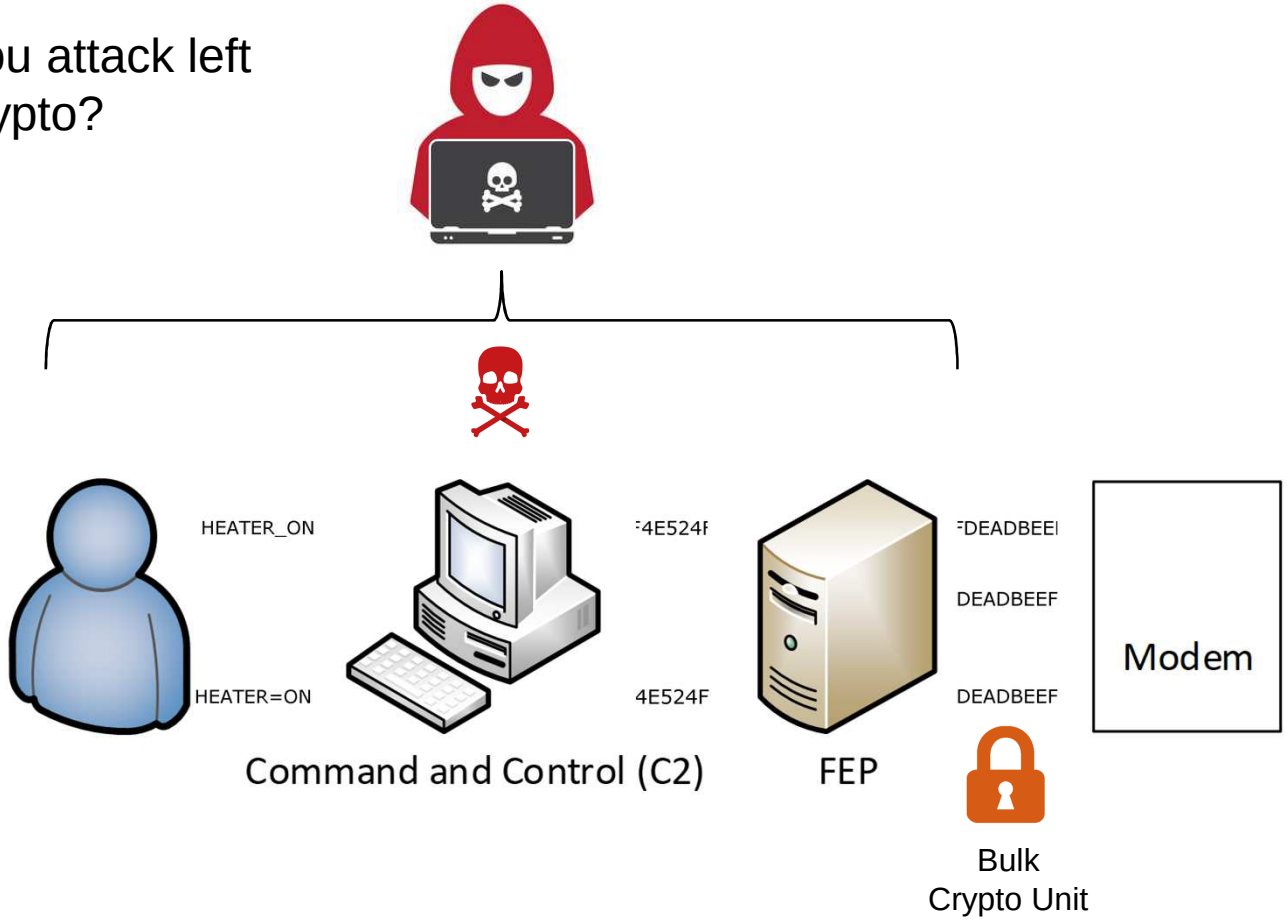
- *Manage cryptographic keys used for encryption and decryption. They generate, store, distribute, and update encryption keys securely to ensure the confidentiality and integrity of communications. Key management practices include key generation, key distribution, key rotation, and key revocation.*

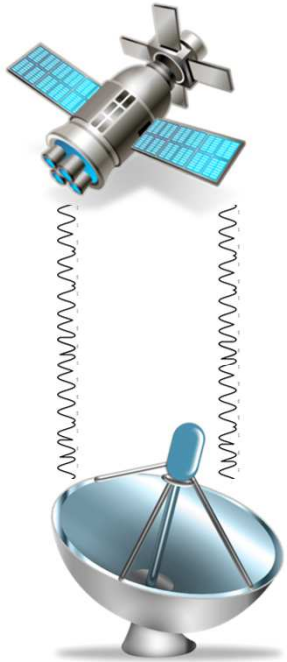
Authentication and Integrity Checking

- *Authentication and integrity checking to verify the identity of communicating entities and ensure the integrity of transmitted data. Authentication mechanisms authenticate the identities of ground systems and spacecraft, while integrity checks detect any unauthorized modifications to the data during transmission.*

hat If….?

Vhat if you attack left
f bulk crypto?

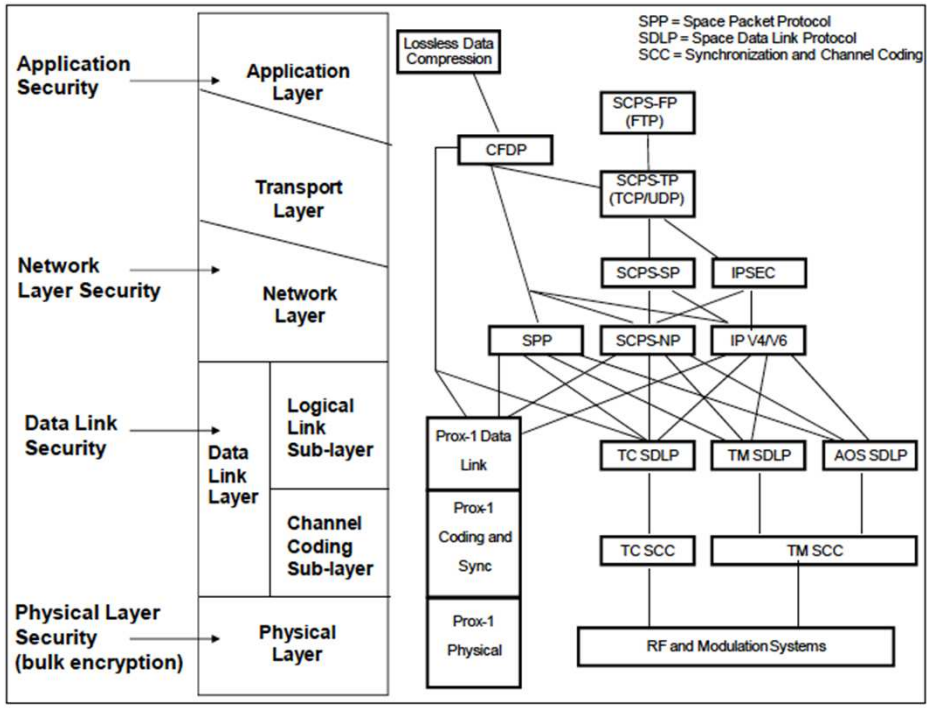




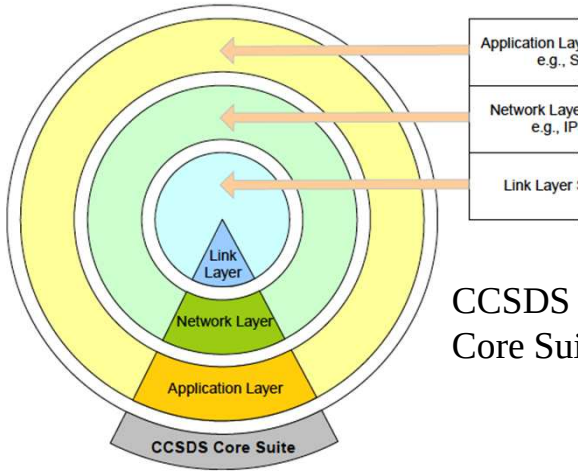
pace Systems Protocol Overview

Many systems use CCSDS as the space systems protocol **– <u>Not everyone does!!!</u>**

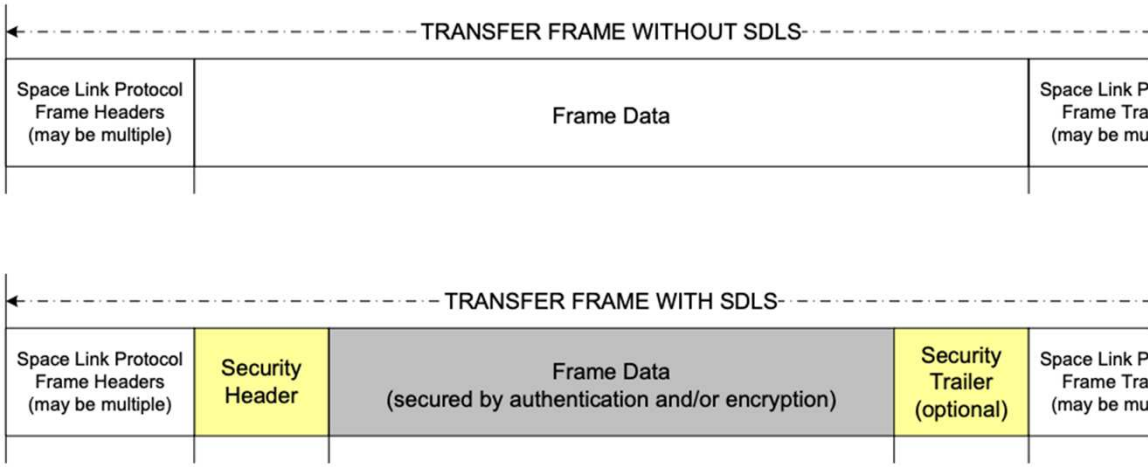
- *Protocols are created by the Consultative Committee for Space Data Systems (CCSDS)*
- *These are recommendations – they are not legally binding*
- *Protocols exist to allow for collaboration between international agencies*
- *Some protocol differences between commands and telemetry*



CCSDS Space Mission Protocols and Security Options

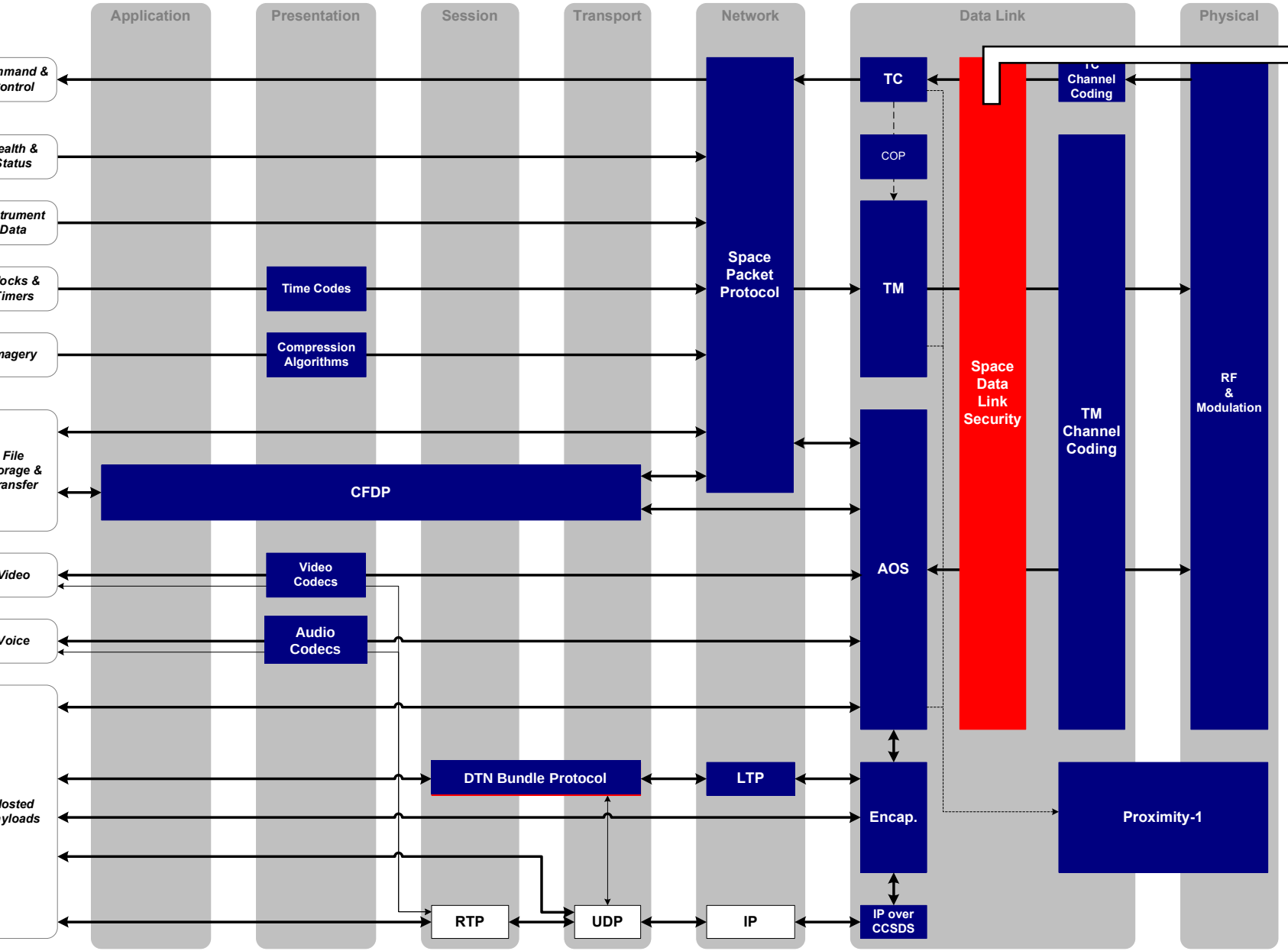


CCSDS
Core Sui



SDLS Blue Book: https://public.ccsds.org/Pubs/355x0b2.pdf

pace-to-Ground: OSI Stack View for CCSDS

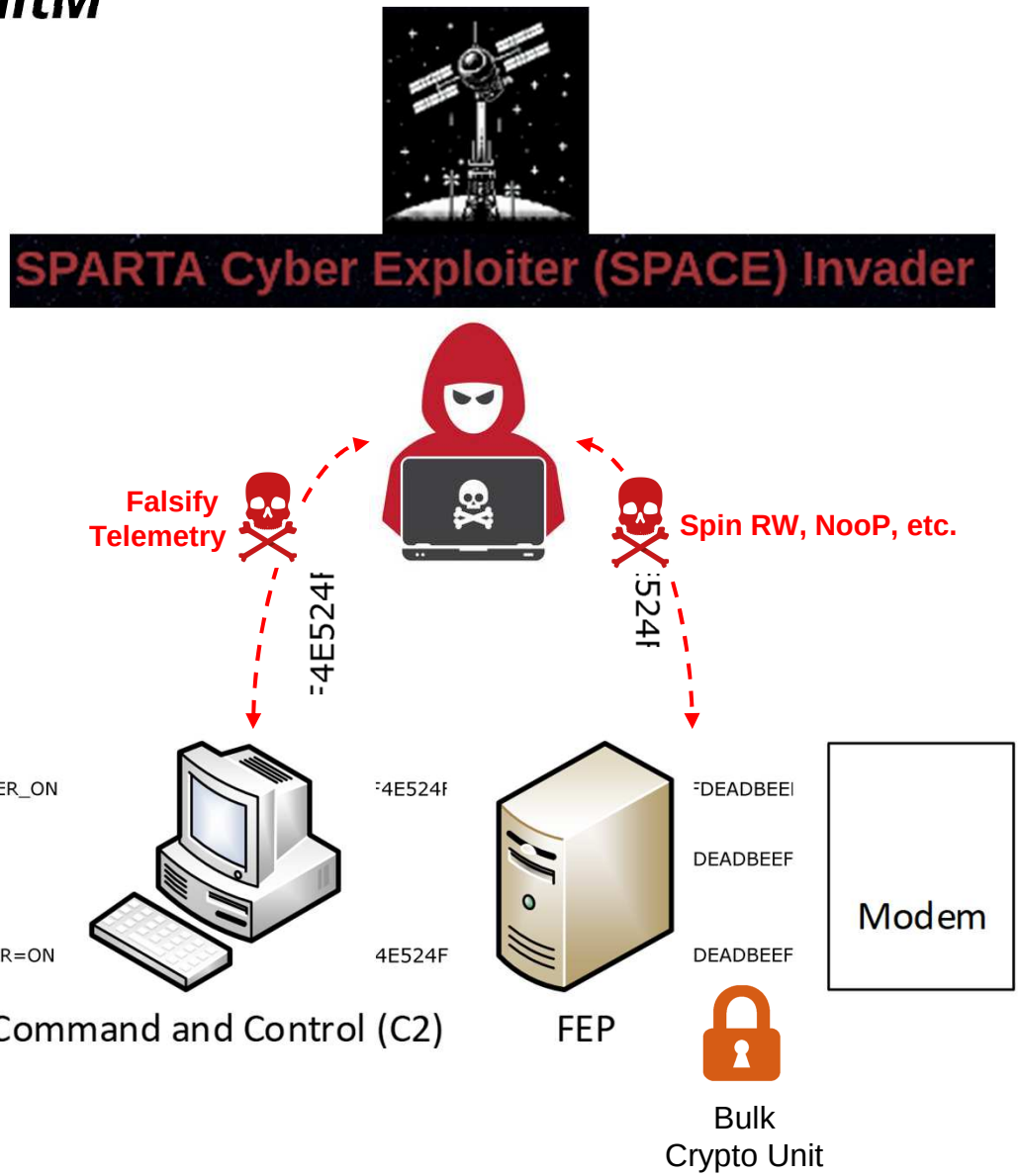


Can support encryptio and authentication

Demo will show why y must do both!!!

Without data link encryption (e.g., SDL replay, injection, evas techniques can be leveraged via Man-in- Middle on the ground

erforming the MitM

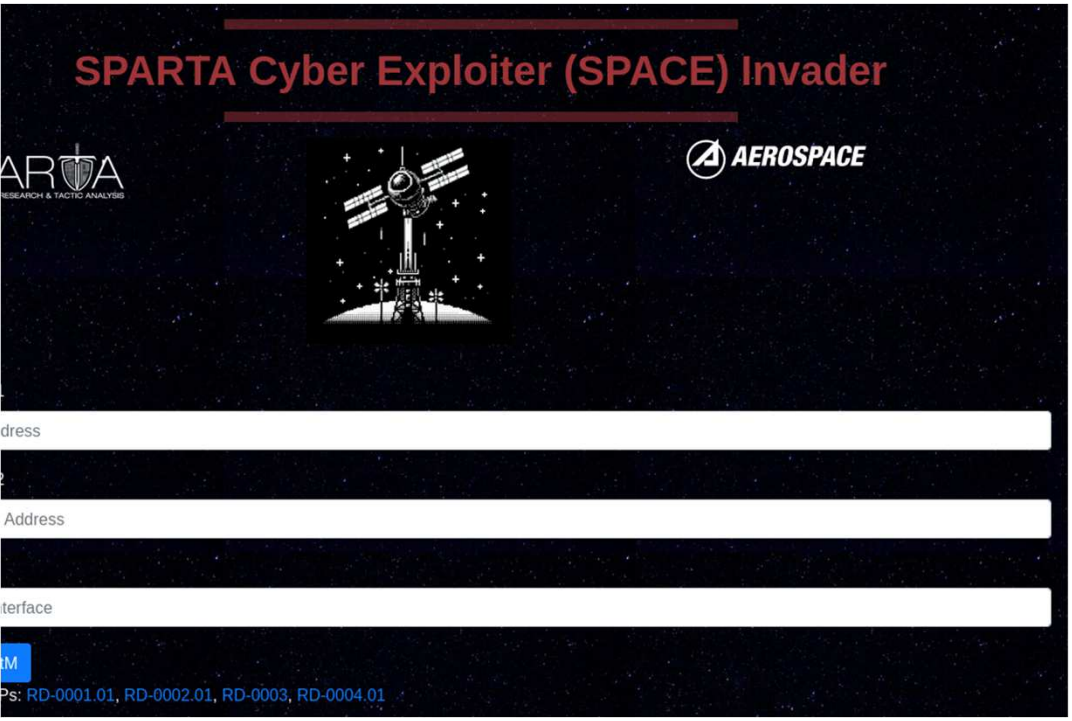


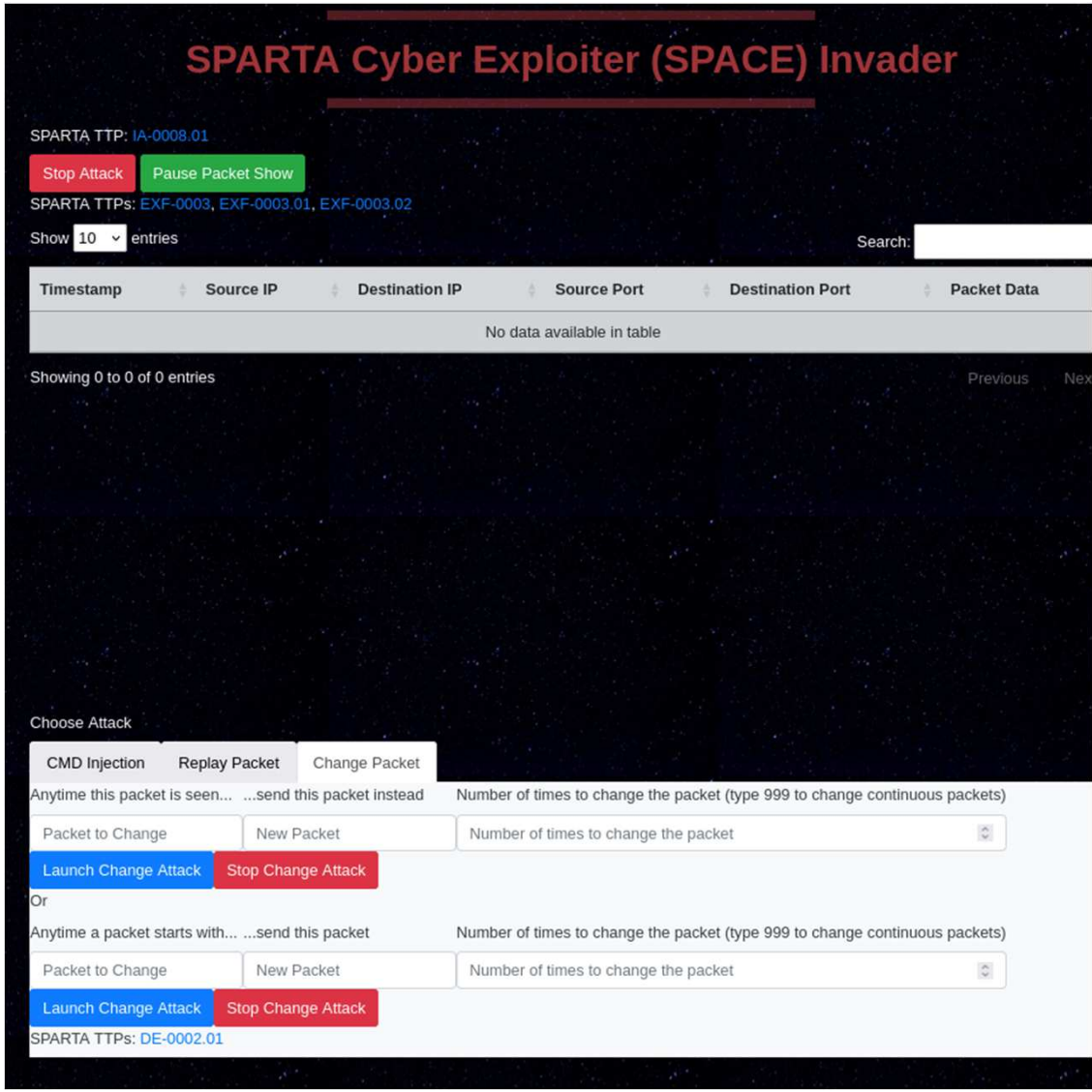
PACE Invader

M Tool / Rogue Ground

PARTA Cyber Exploiter (SPACE) Invader

- Acts as a rogue ground station or performs MitM attacks
- Currently utilizes 12 SPARTA TTPs
- Parsers for numerous open-source ground station CMD/TLM databases

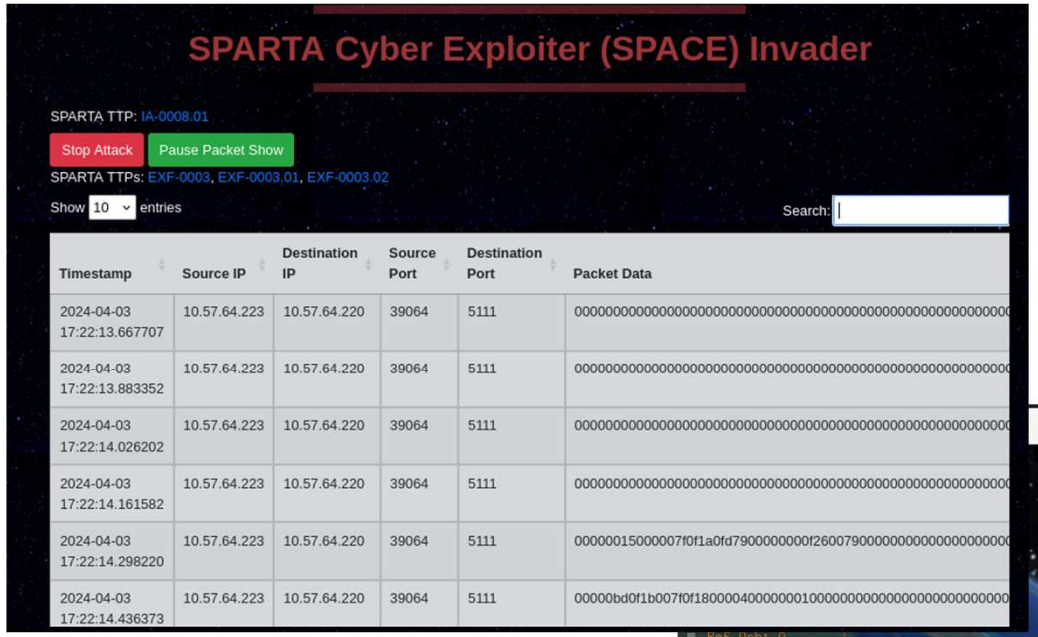


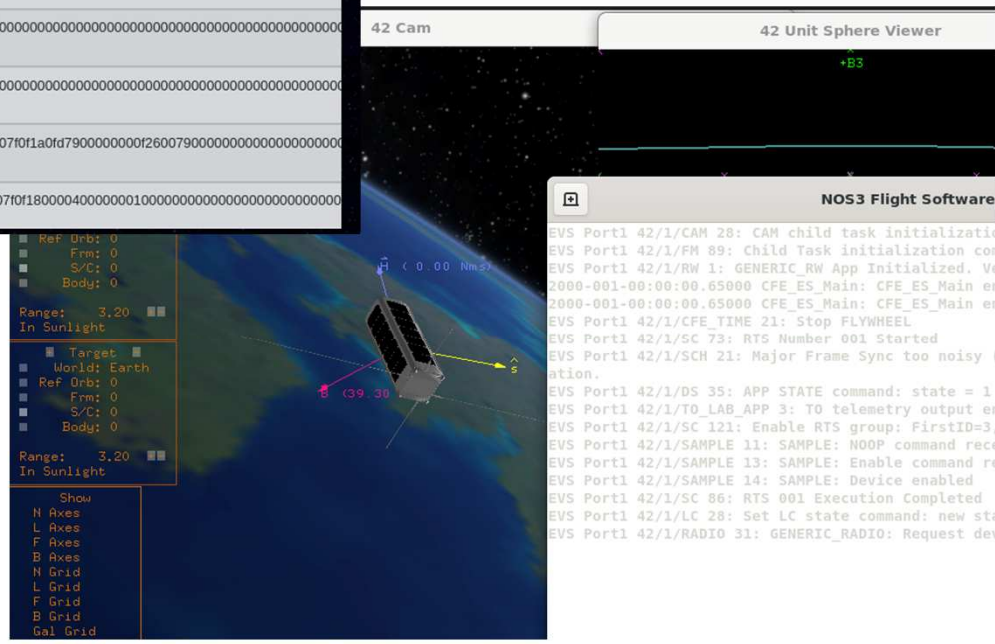


PACE Invader (cont.)

pes of attacks available (for now)

- Exfiltrating data
- Falsify telemetry
- Ability to replay commands
- Ability to send commands
- Jamming
- Flooding
- Rogue Ground Station
- Rogue Flight Application
- Etc.



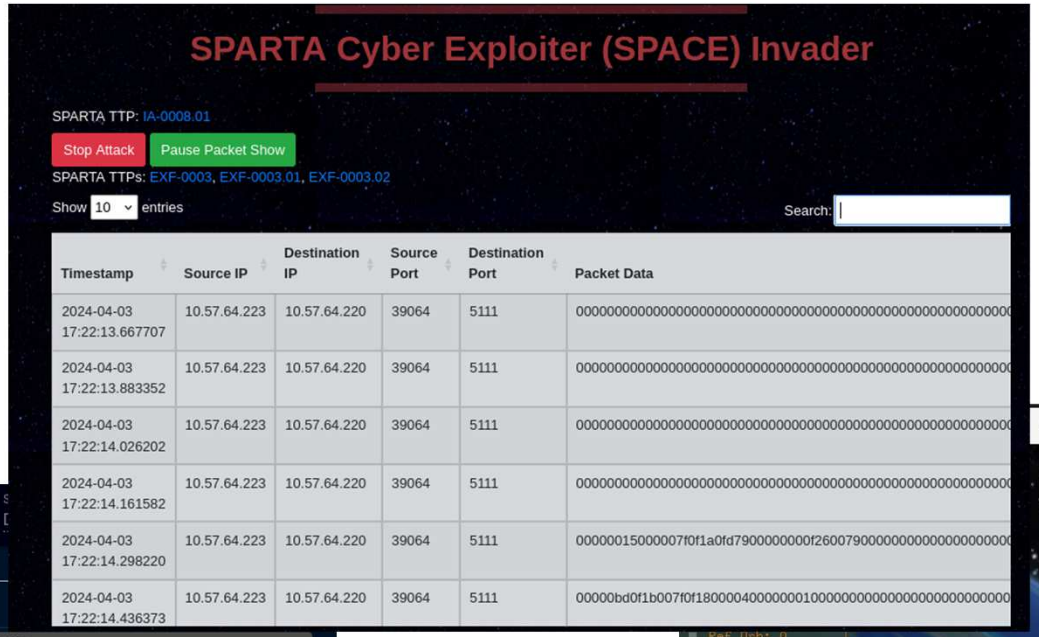


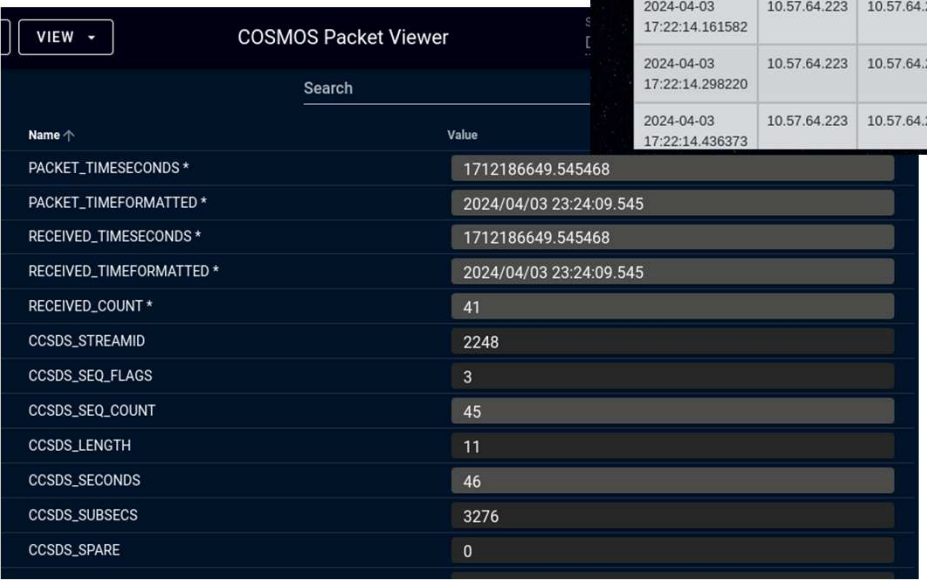
mo Time!!!

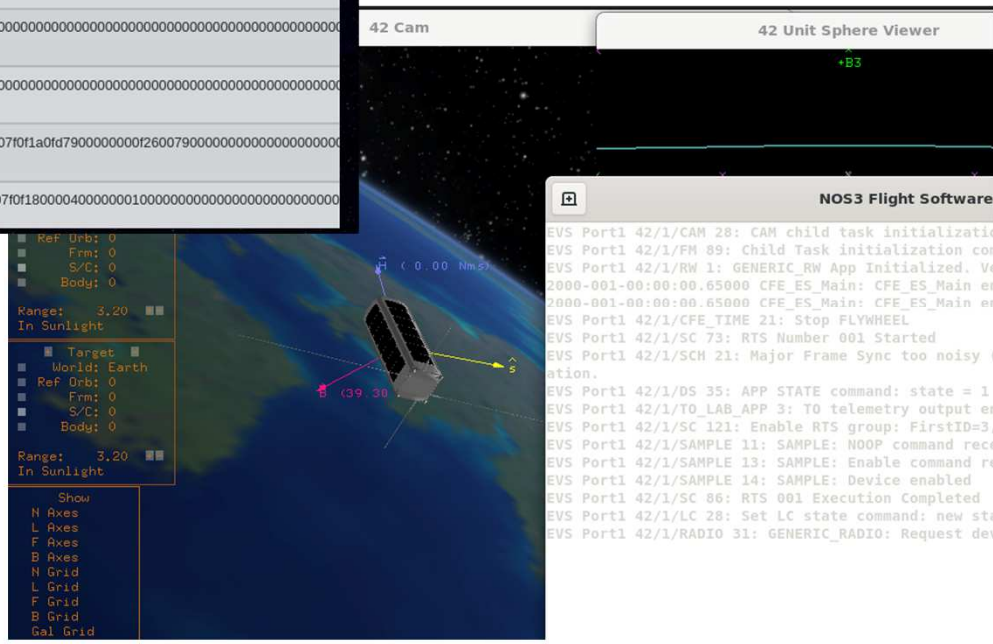
https://github.com/nasa/nos

cenario #1 – No SDLS

- Exfiltrating data
- Falsify telemetry
- Ability to replay commands
- Ability to send commands
- Etc.





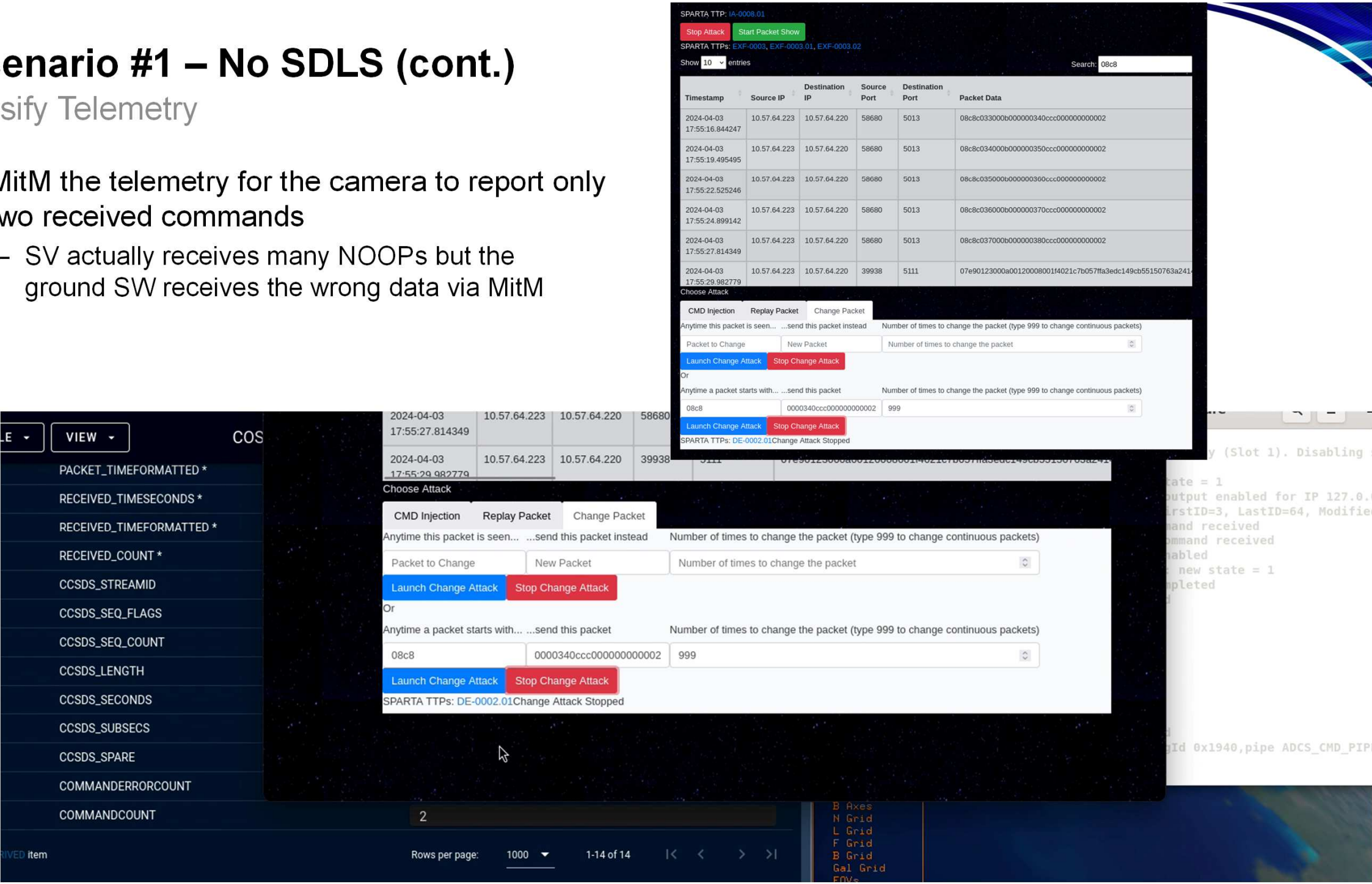


https://github.com/nasa/nos

enario #1 – No SDLS (cont.)

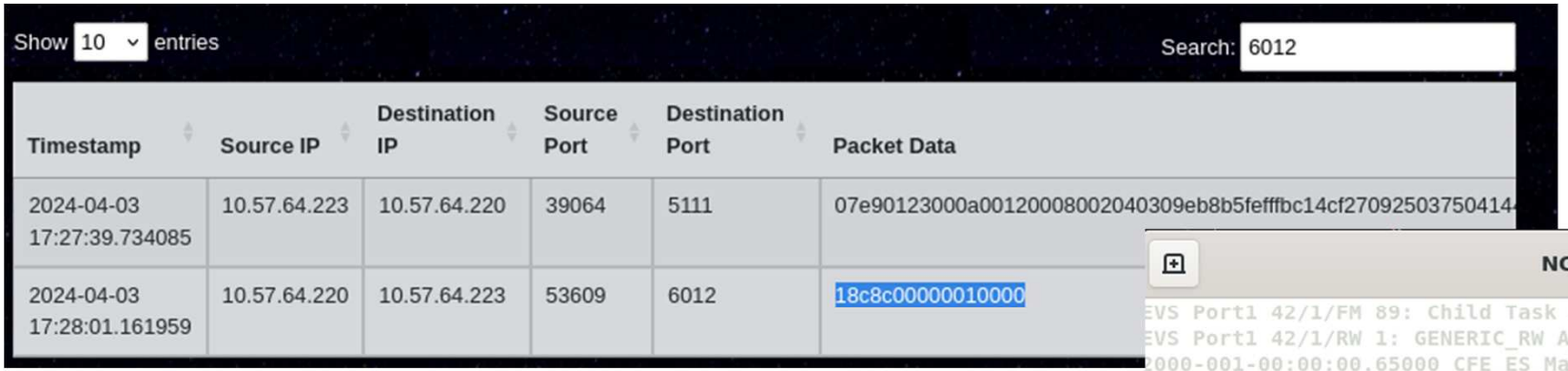
sify Telemetry

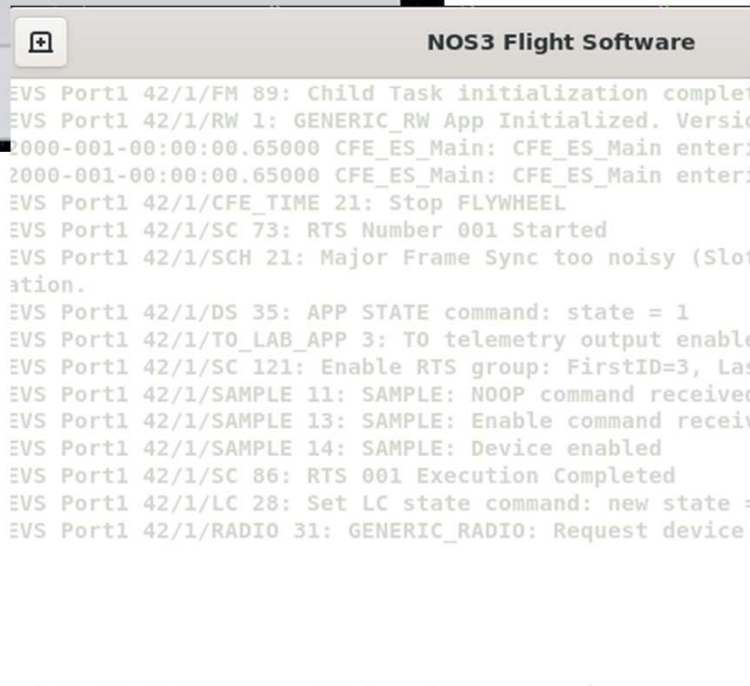
- MitM the telemetry for the camera to report only two received commands
  - SV actually receives many NOOPs but the ground SW receives the wrong data via MitM



cenario #1 – No SDLS (cont.)

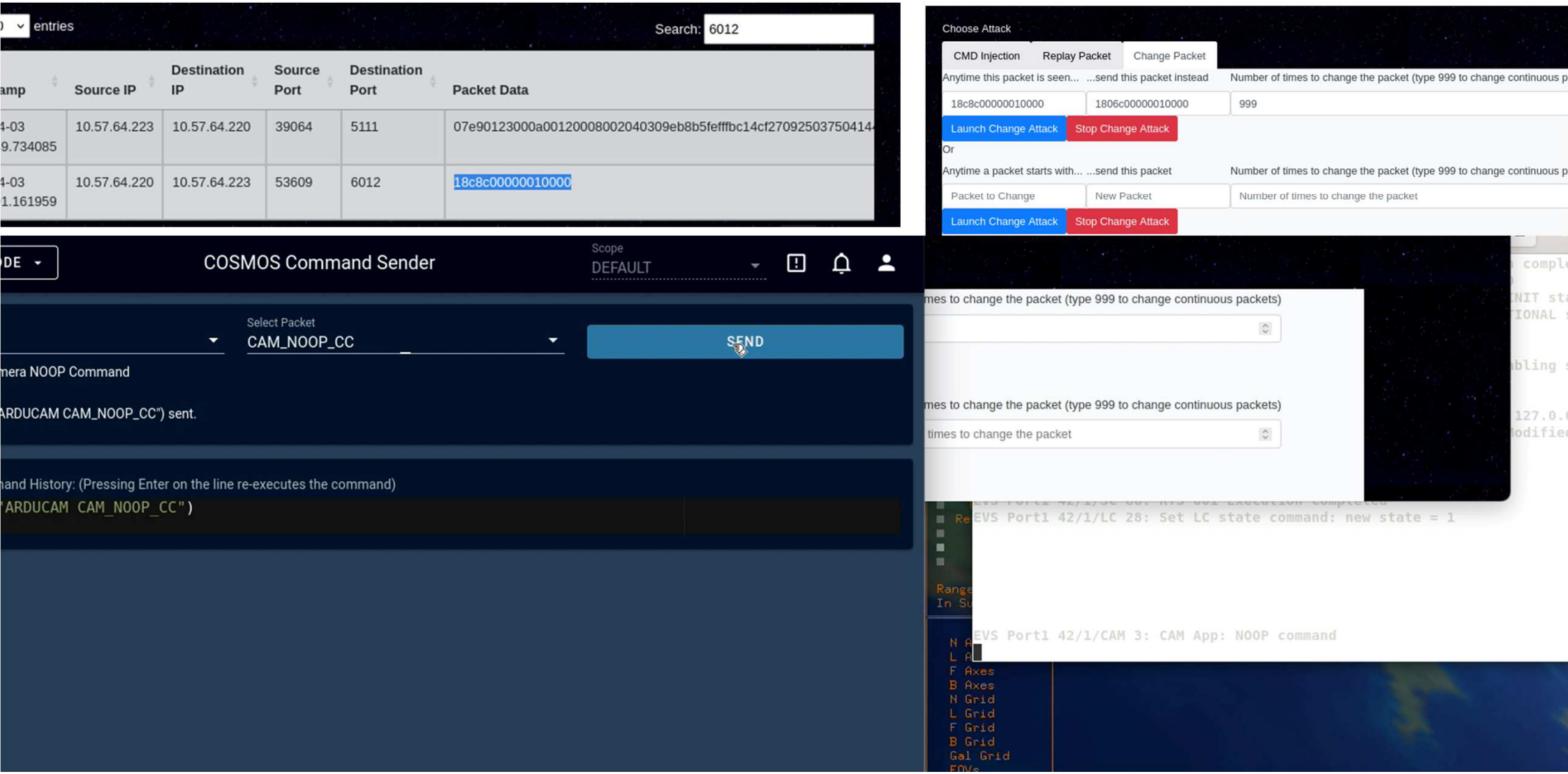
Monitoring the traffic, you see a Camera NOOP go to the SV; what if we change it the next time and every time moving forward?





cenario #1 – No SDLS (cont.)

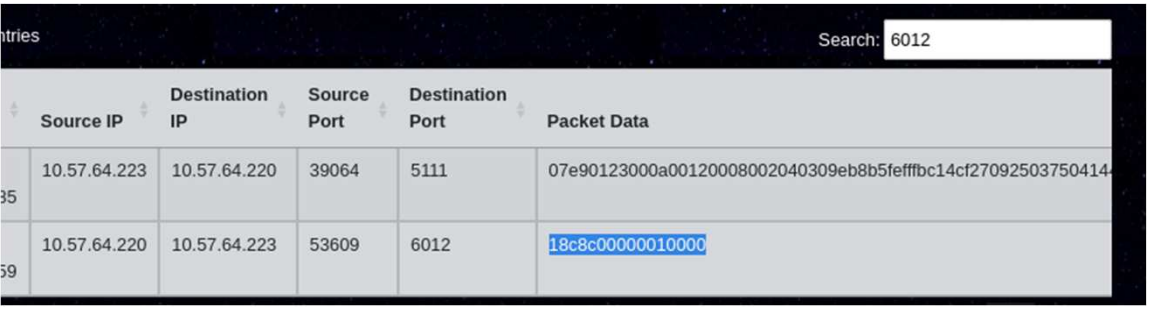
MitM every time a CAM_NOOP_CC goes across the wire and change it to a CFS ES NOOP

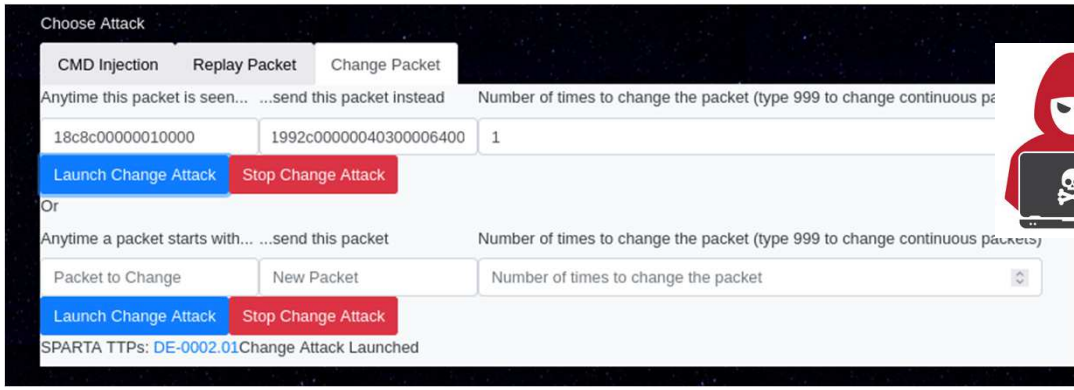


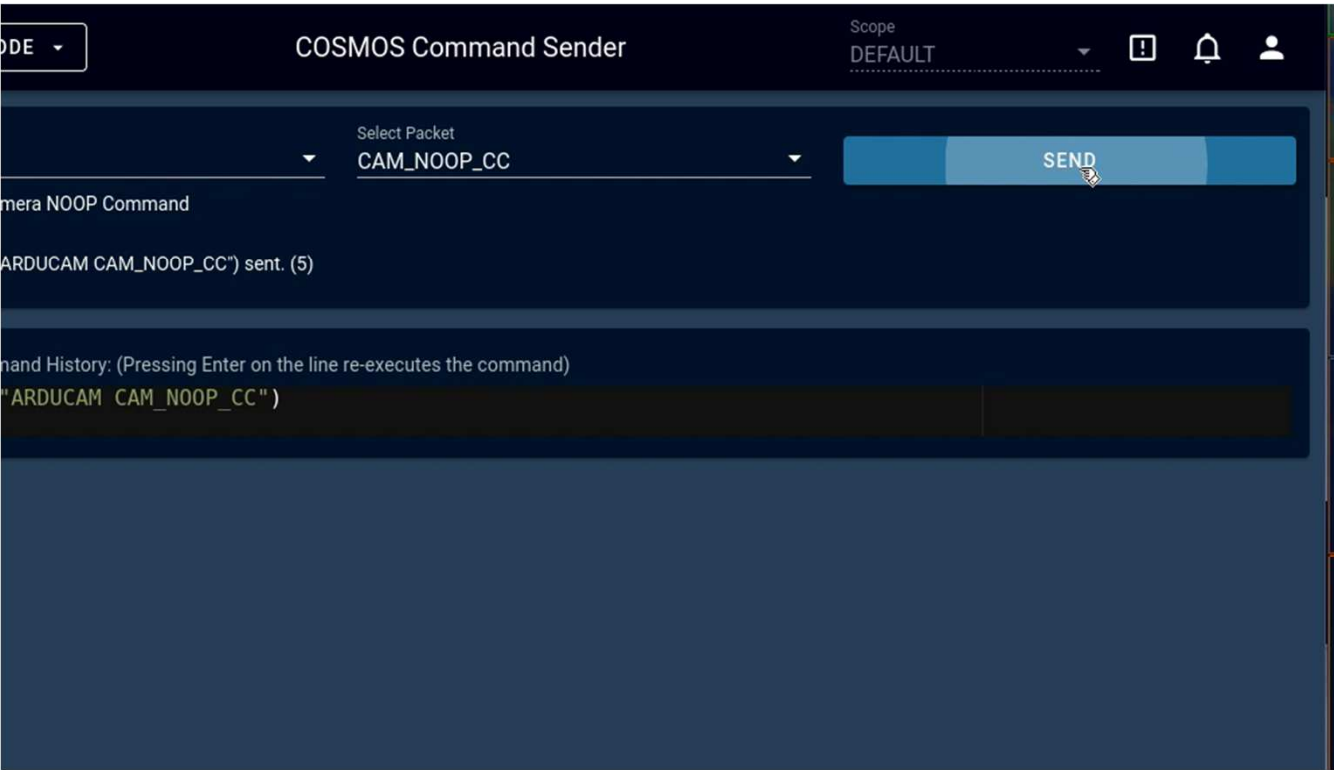
cenario #1 – No SDLS (cont.)

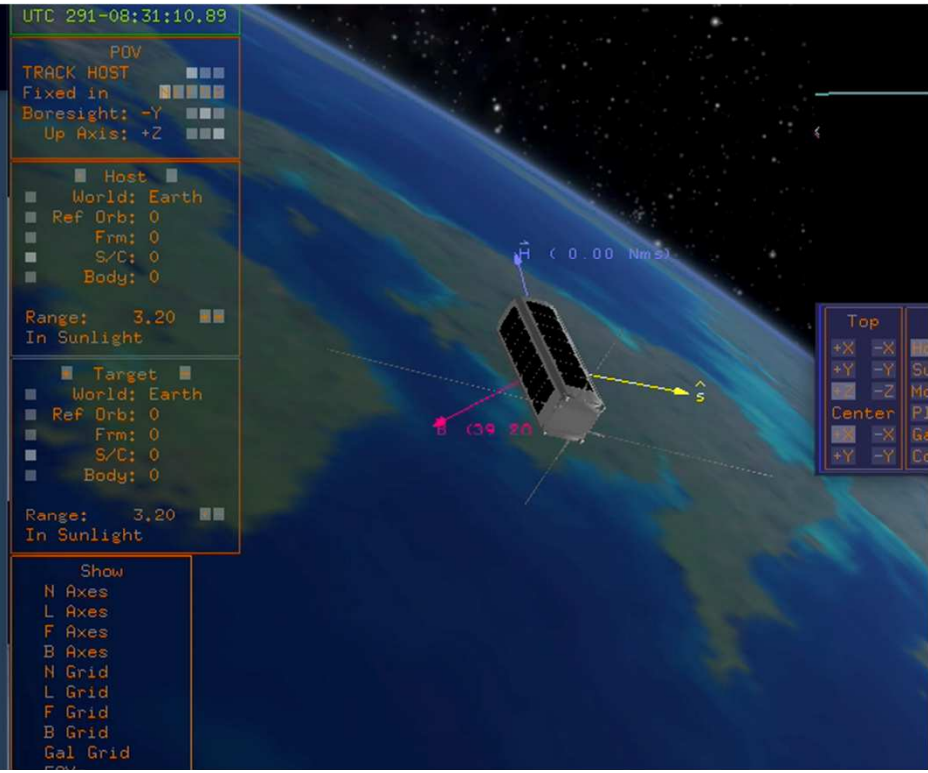
OOPs Are Fun….but Let's Make It Spin!!!

MitM the next CAM_NOOP_CC to spin the reaction wheels to cause an uncontrollable spin







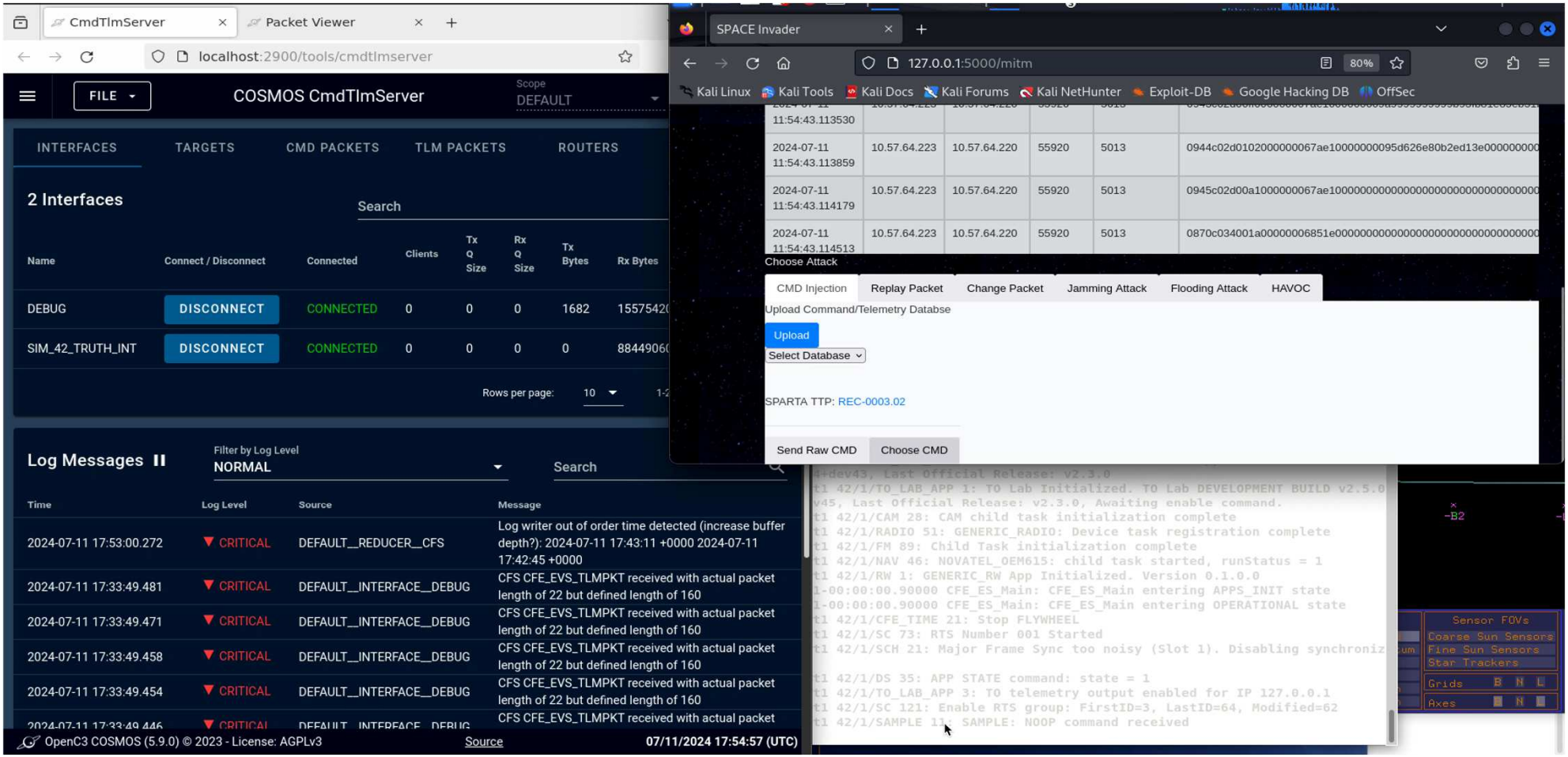


cenario #1 – No SDLS (cont.)

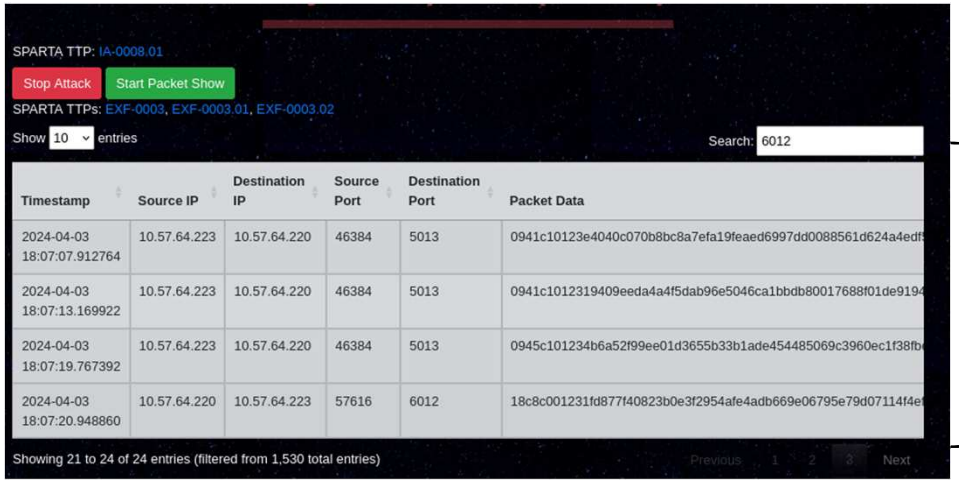
an do everything you can do, but better with Rogue Ground Station

Find the command database and load it into the tool

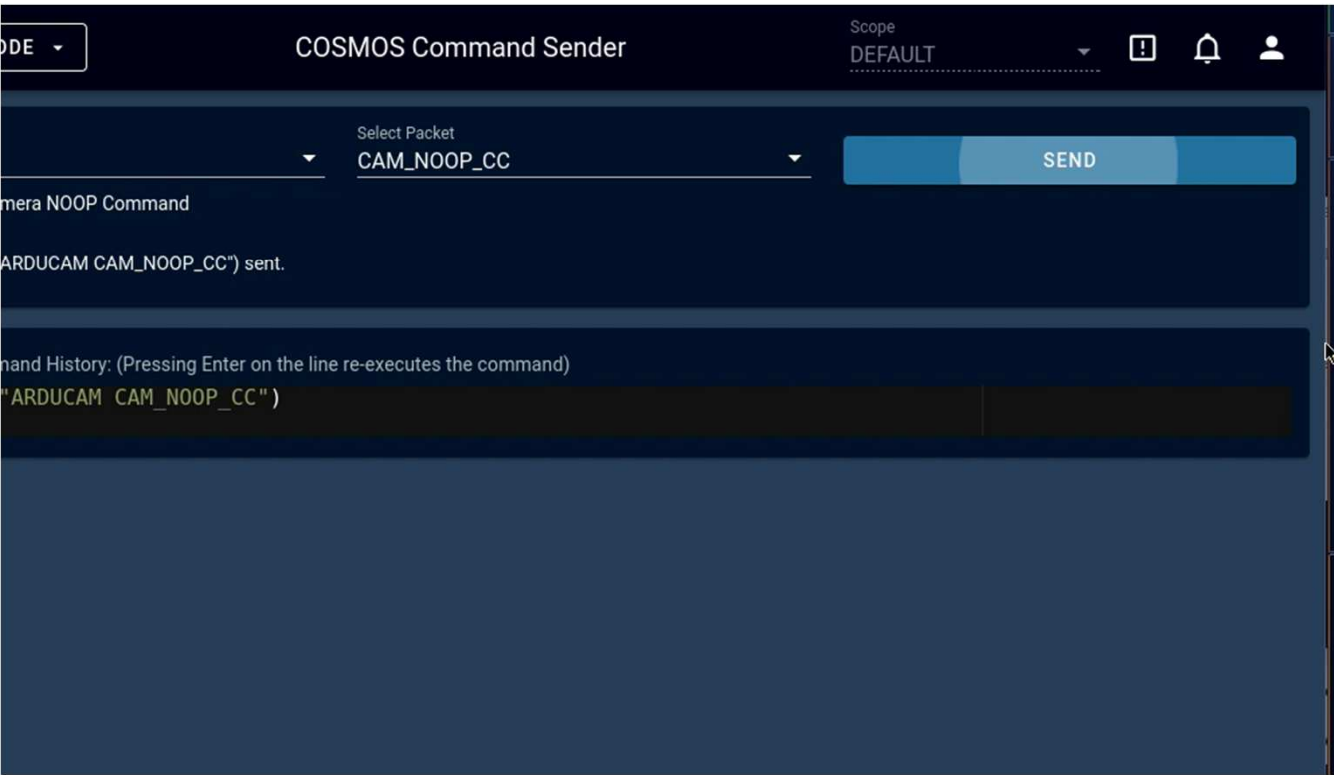
Deploy commands as a normal operator

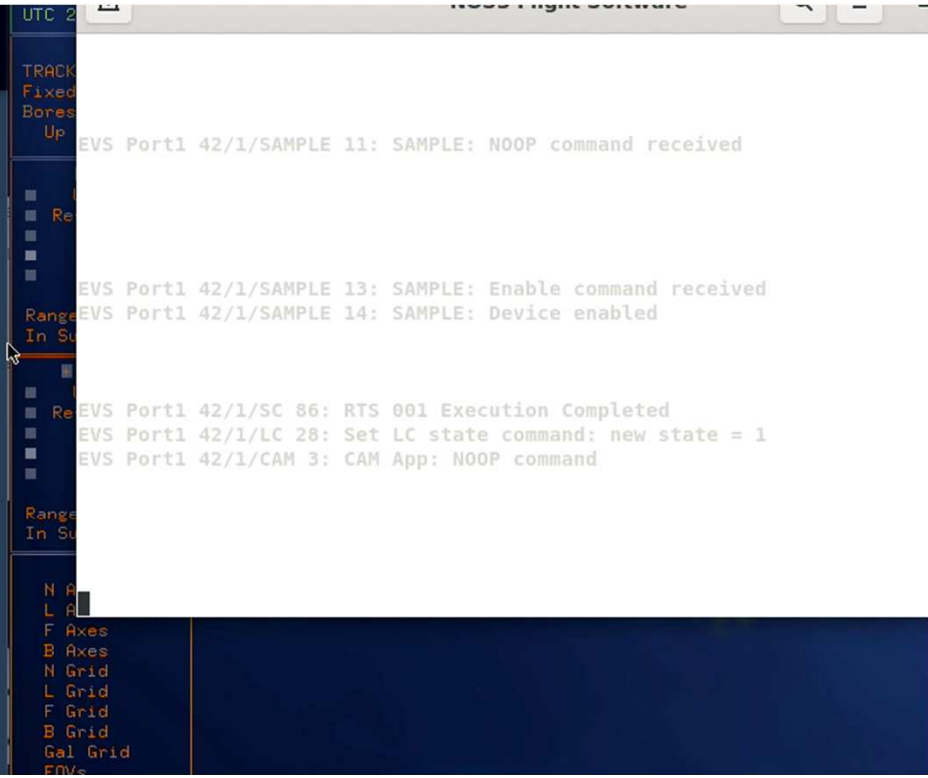


cenario #2 – With SDLS Using Only Encryption



Data looks different now…

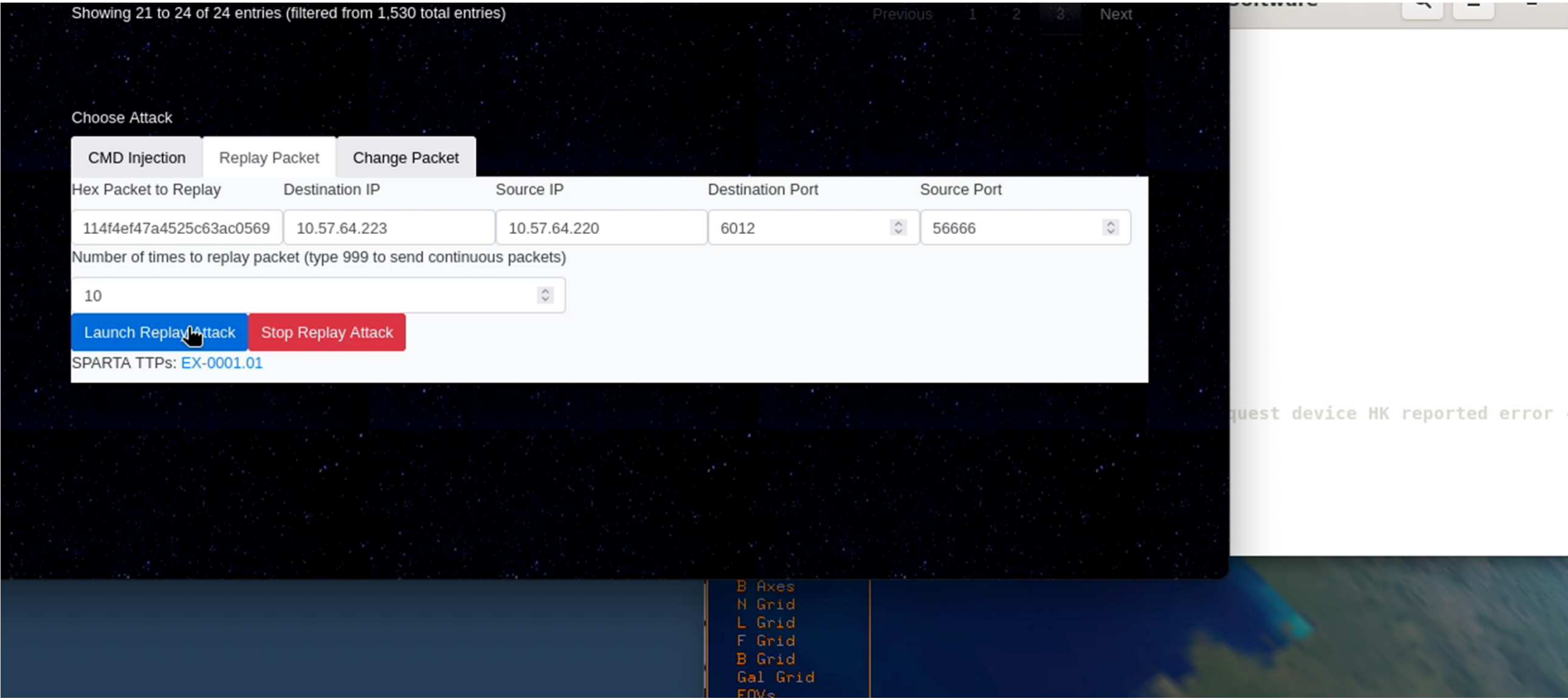




cenario #2 – With SDLS Using Only Encryption

play Attack Still in Play!!

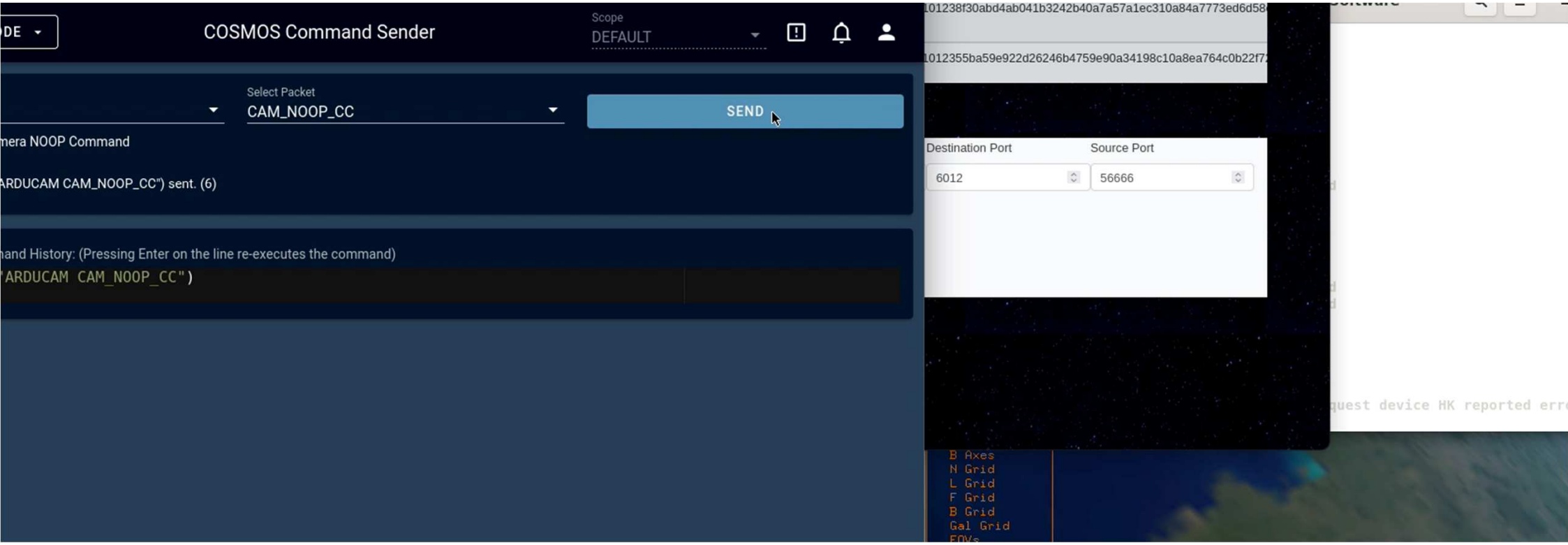
Without sequencing, command counters, authentication of some sort – replay attacks will still work



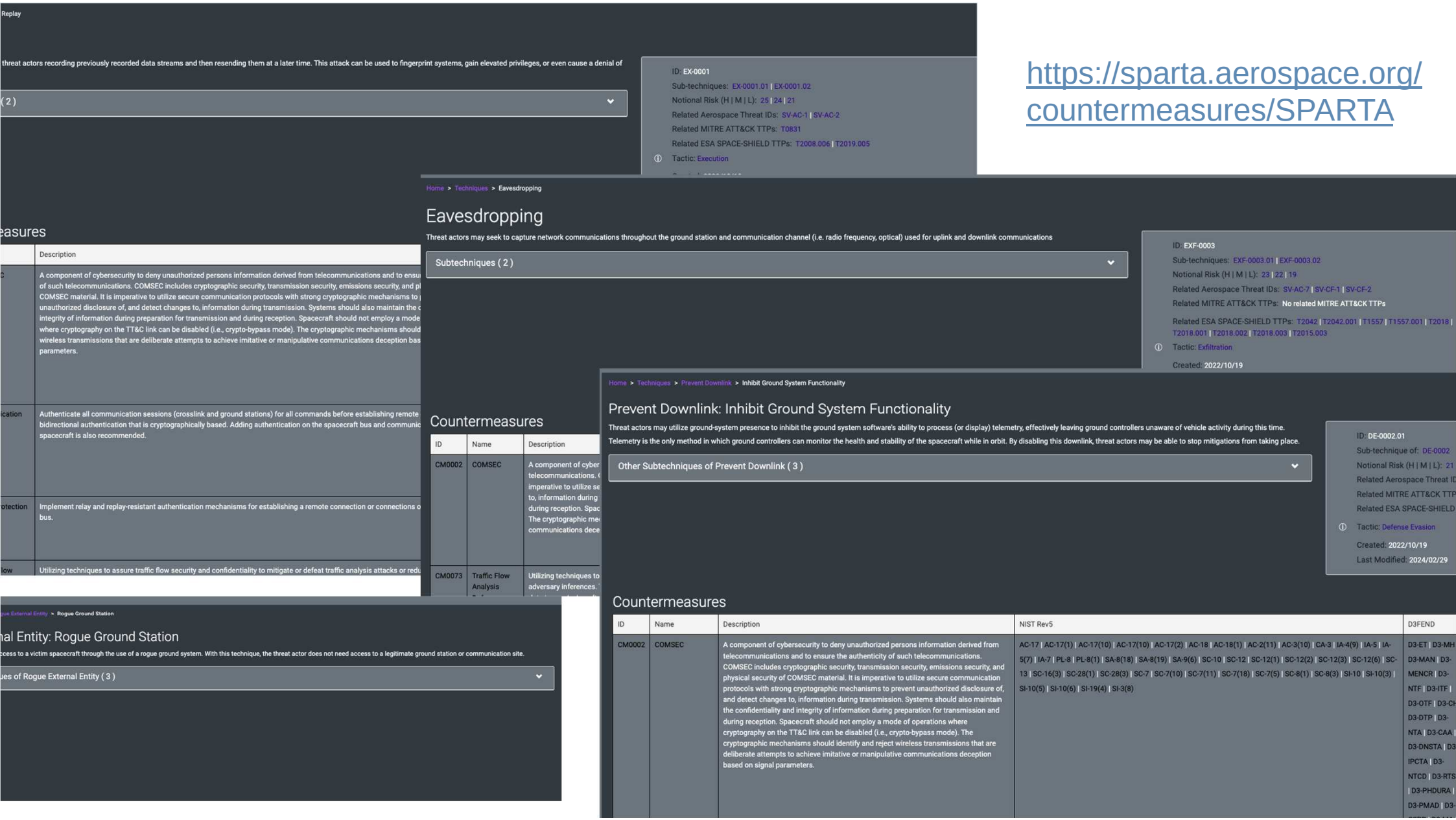
cenario #3 – With SDLS Using Encryption & Authentication

ne of the Previous Attacks Work ☹

Attempt to perform command injection, replay, etc. – nothing works



chniques Used >>> SPARTA Countermeasures



https://sparta.aerospace.org/countermeasures/SPARTA

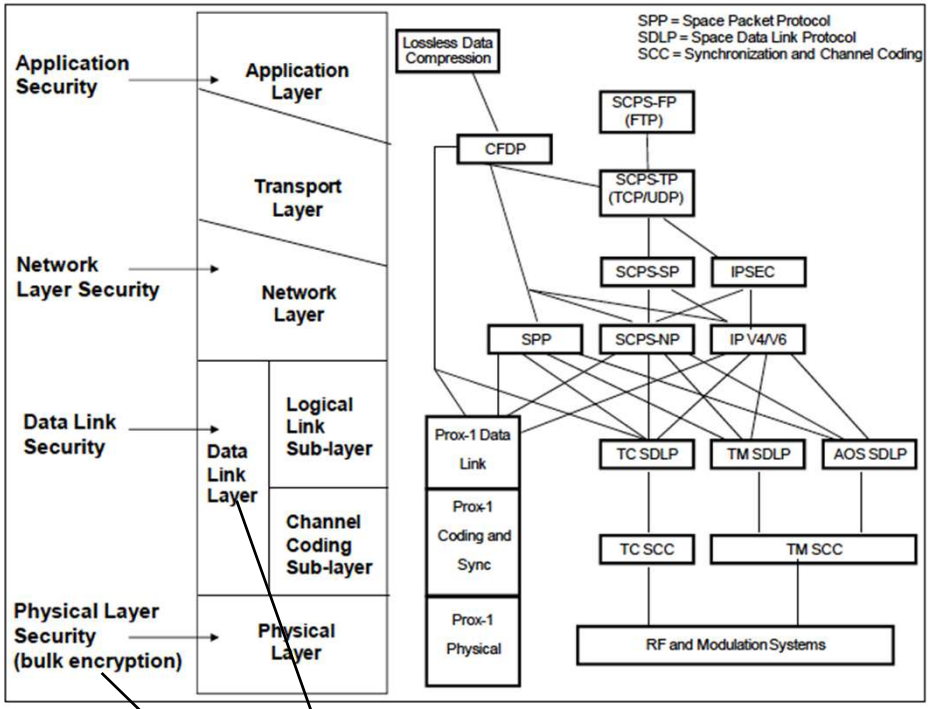
ummary

k is Good – Both is Better!!!

cording to SPARTA Notional Risk Scores

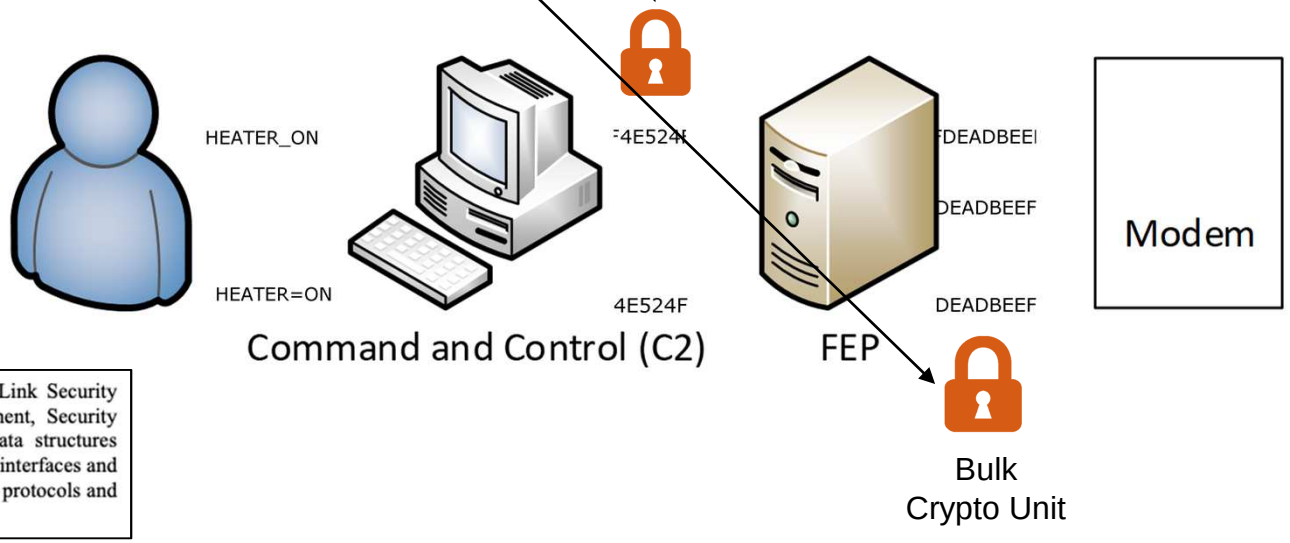
Compromised ground is one of the highest risks to the SV

SPARTA Techniques/Sub-Techniques	Notional Risk (HIGH Criticality Systems)
IA-0004.01 - Ground Station	25
IA-0008.01 - Rogue Ground Station	25
PER-0003 - Ground System Presence	25
EXF-0007 - Compromised Ground System	25
IA-0007 - Compromise Ground System	24



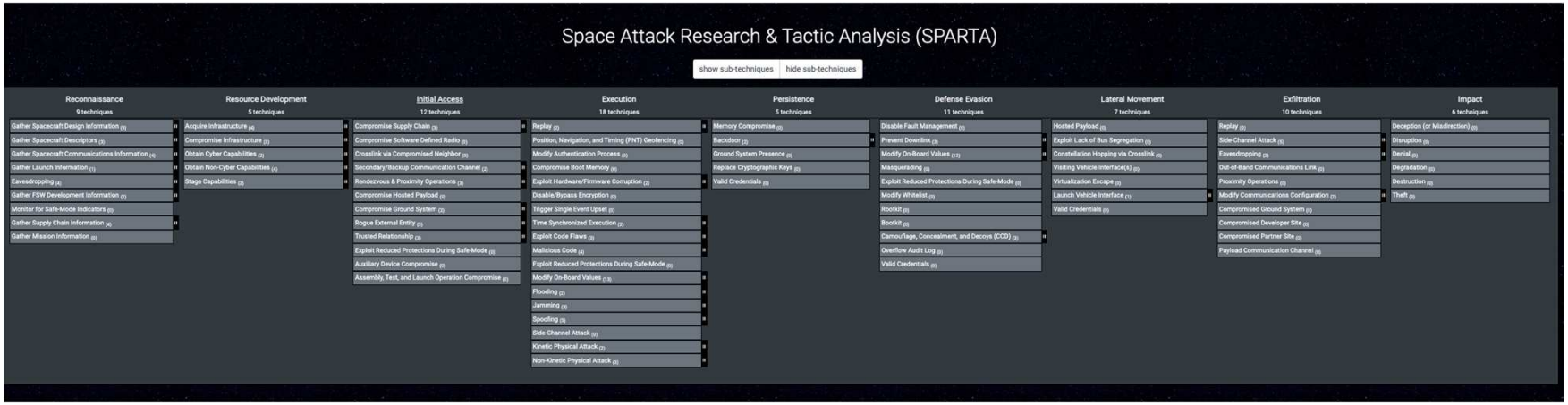
Adding defense-in-depth is key!!!

- If using CCSDS (TC/TM/AOS) SDLS improves security immensely and mitigates many known TTPs
  - SDLS Extended Procedures are also available



purpose of this Recommended Standard is to specify the Space Data Link Security LS) Protocol Extended Procedures (EP). It defines the Key Management, Security ociation Management, SDLS Monitoring and Control Services, and data structures ired to operate the SDLS protocol over a space link. Further, it defines the interfaces and ired data structures for proper interaction with the Space Data Link (SDL) protocols and curity function status reporting mechanism.

https://sparta.aerospace.org



ple Media Links:

ps://cyberscoop.com/space-satellite-cybersecurity-sparta/
ps://www.darkreading.com/ics-ot/space-race-defenses-satellite-perattacks
ps://thecyberwire.com/podcasts/daily-podcast/1715/notes &
ps://thecyberwire.com/newsletters/signals-and-space/6/21

Overview Briefings:

- Using SPARTA to Conduct Space Vehicle Cyber Assessments (February 2024)
- DEF CON 31: Building Space Attack Chains using SPARTA (August 2023)
- Hacking Spacecraft using Space Attack Research & Tactic Analysis | Video (April 2023
- In-depth Overview - Space Attack Research & Tactic Analysis (November 2022)

SPARTA Links:

Getting Started with SPARTA: https://sparta.aerospace.org/resources/getting-started | https://sparta.aerospace.org/resources/
Understanding Space-Cyber TTPs with the SPARTA Matrix: https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix
Leveraging the SPARTA Matrix: https://aerospace.org/article/leveraging-sparta-matrix
Use Case w/ PCspooF:

- https://aerospacecorp.medium.com/sparta-cyber-security-for-space-missions-4876f789e41c
- https://medium.com/the-aerospace-corporation/a-look-into-sparta-countermeasures-358e2fcd43ed

FAQ: https://sparta.aerospace.org/resources/faq
Matrix: https://sparta.aerospace.org
Navigator: https://sparta.aerospace.org/navigator | Countermeasure Mapper: https://sparta.aerospace.org/countermeasures/mapper
Notional Risk Scores on 5x5: https://sparta.aerospace.org/notional-risk-scores
Related Work: https://sparta.aerospace.org/related-work/did-space with ties into TOR 2021-01333 REV A

her Papers and Resources

CYSAT '23:
https://www.youtube.com/watch?v=l9nezXxO3iE

- SPARTA (SPACE ATTACK RESEARCH & TACTIC ANALYSIS) https://sparta.aerospace.org/resources/

- DEF CON Presentations:
  - DEF CON 2020: Exploiting Spacecraft
  - DEF CON 2021: Unboxing the Spacecraft Software BlackBox Hunting for Vulnerabilities
  - DEF CON 2022: Hunting for Spacecraft Zero Days using Digital Twins
  - DEF CON 2023: Building Space Attack Chains using SPARTA

DEFCON AEROSPACE VILLAGE

- Papers/Articles: https://aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368
  - 2019: Defending Spacecraft in the Cyber Domain
  - 2020: Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices
  - 2021: Cybersecurity Protections for Spacecraft: A Threat Based Approach
  - 2021: The Value of Space
  - 2021: Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles
  - 2022: Protecting Space Systems from Cyber Attack
  - 2022: An International Technical Standard for Commercial Space System Cybersecurity - A Call to Action

- July 2022 Testimony: Space and Aeronautics Subcommittee Hearing - Exploring Cyber Space: Cybersecurity for Civil and Commercial Space Systems
  - Video: https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964
  - Written Testimony: https://republicans-science.house.gov/_cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf

COMMITTEE ON SCIENCE AND SPACE AND TECHNOL