DefCon 32: Aerospace Village
From Theory to Reality: Demonstrating the Simplicity of SPARTA Attacks

Randi Tinney, Brandon Bailey

Cybersecurity and Advanced Platforms Subdivision (CAPS)
Cyber Assessment & Research Dept (CARD)
The Aerospace Corporation

randi.j.tinney@aero.org

Approved for Public Release via OTR-2024-00993

About Me

Randi Tinney

- Previously was an Cybersecurity Engineer at NASA's Independent Verification and Validation Center
- Currently an Engineering Specialist at the Aerospace Corporation
  - Vulnerability Researcher and Exploit Developer
    - Specialize Ground Systems and Spacecraft Systems
  - Perform Penetration Testing and Vulnerability Assessments
    - James Web Telescope (JWST) Ground System and Space Telescope Science Institute (STScI) in Baltimore
    - Huntsville Operations Support Center (HOSC) at Marshall Space Flight Center
    - Near Earth Network (NEN) at Wallops Flight Center
    - Space Network (SN) at White Sands Complex (WSC)
    - Moonlighter (Hack-a-Sat)
  - Helped develop the Space Attack Research & Tactic Analysis (SPARTA) Framework
- Member of team that won a Black Badge at DEFCON 31 from the Red Alert ICS CTF

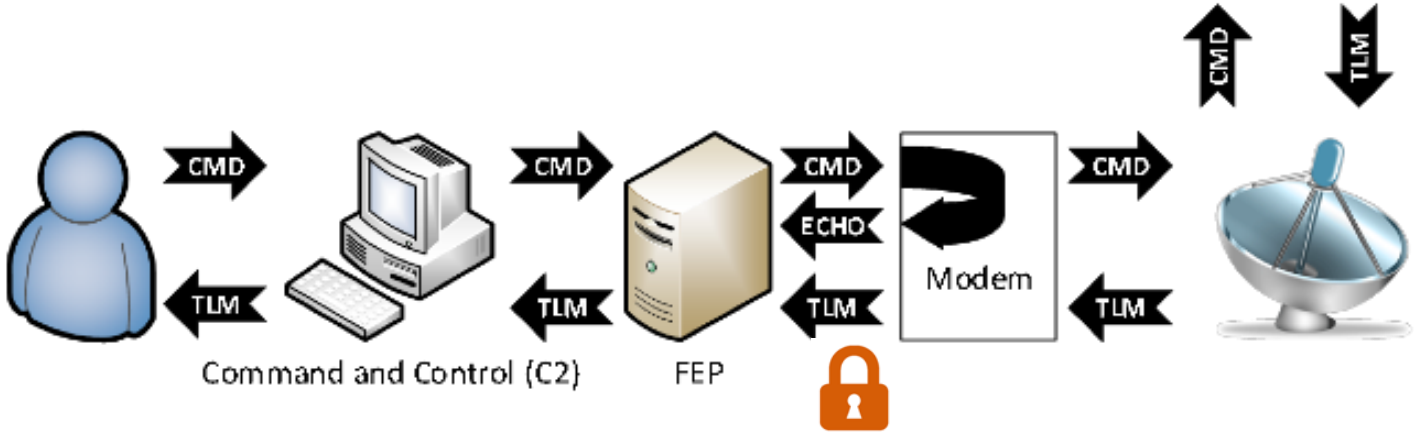
Space Attack Research & Tactic Analysis (SPARTA) – Launched October 2022

Filling the TTP Gap for Space

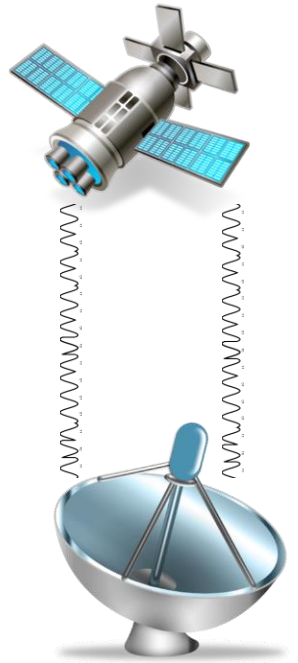
- Cybersecurity matrices are industry-standard tools and approaches for commercial and government users to navigate rapidly evolving cyber threats and vulnerabilities and outpace cyber threats
  - They provide a critical knowledge base of adversary behaviors
  - Framework for adversarial actions across the attack lifecycle with applicable countermeasures
- Current cybersecurity matrices (including MITRE ATT&CK) are limited to ground systems which lead to a gap!
- **Aerospace's SPARTA is the first-of-its-kind body of knowledge on cybersecurity protections for spacecraft and space systems, filling a critical vulnerability gap exists for the U.S. space enterprise**

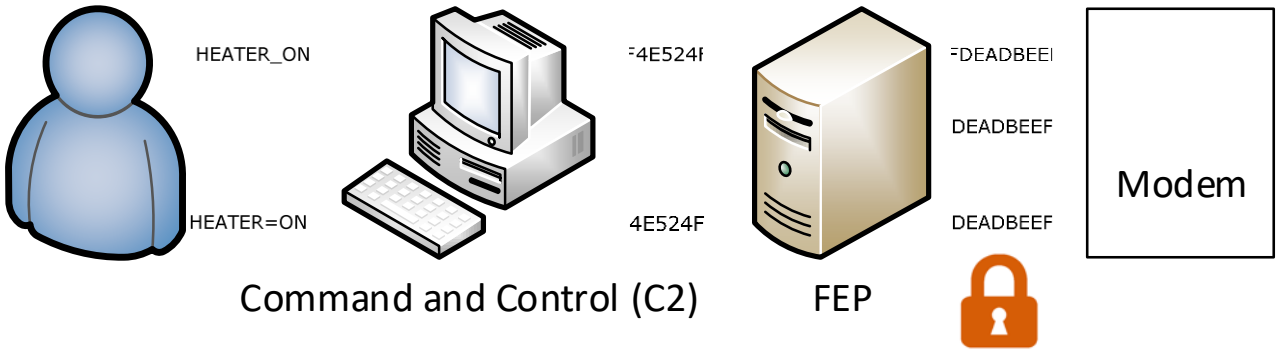
SPARTA provides unclassified information to space professionals about how spacecraft may be compromised

Basics: Commanding & Telemetry



Bulk
Crypto Unit

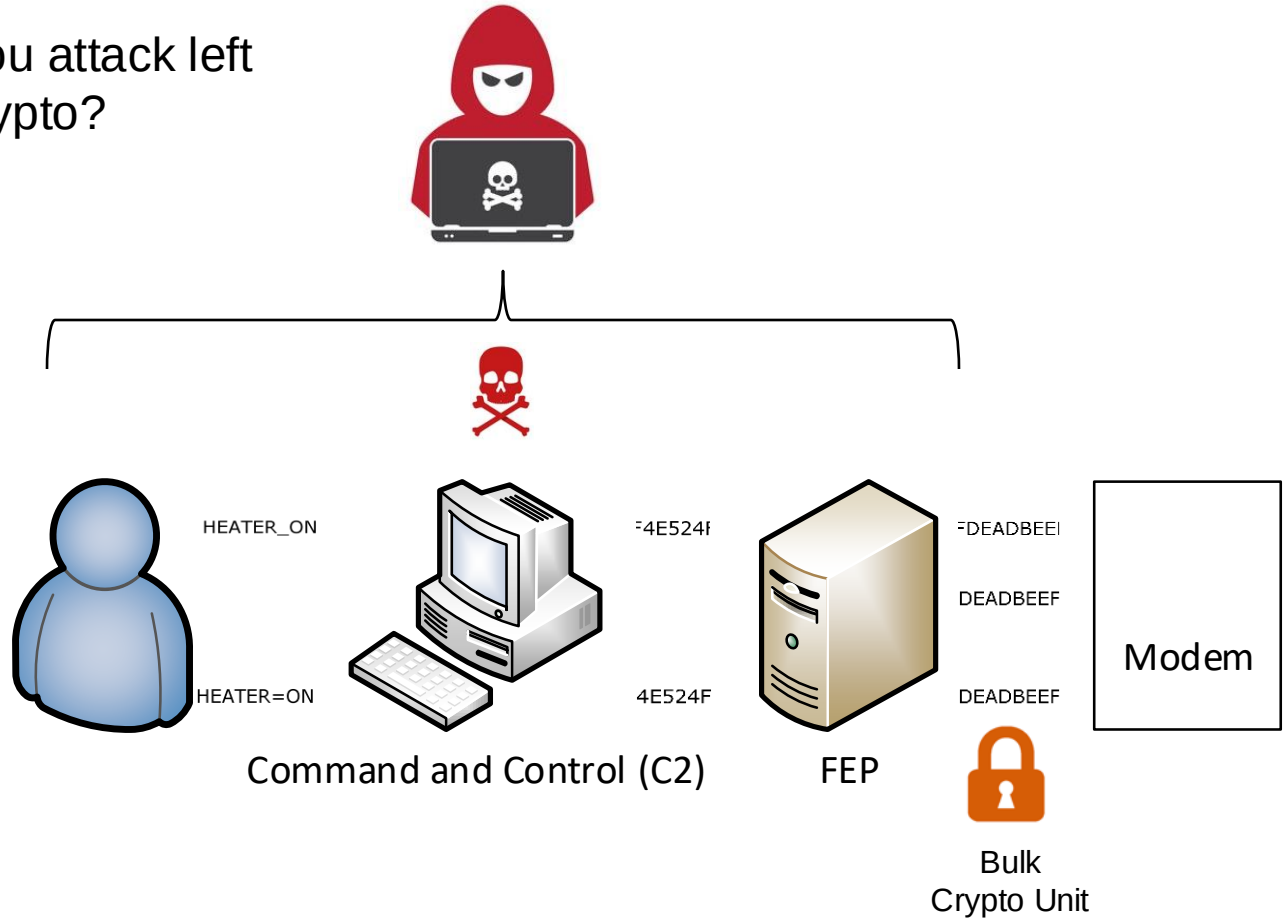


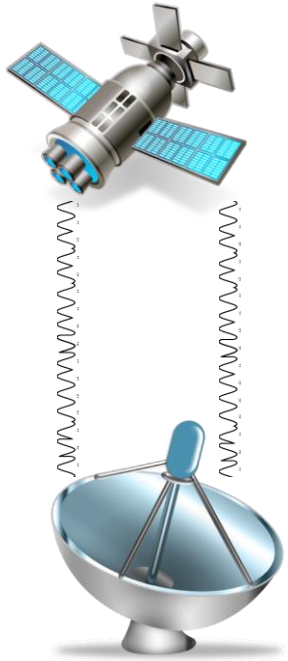


Bulk
Crypto Unit

What If….?

What if you attack left of bulk crypto?

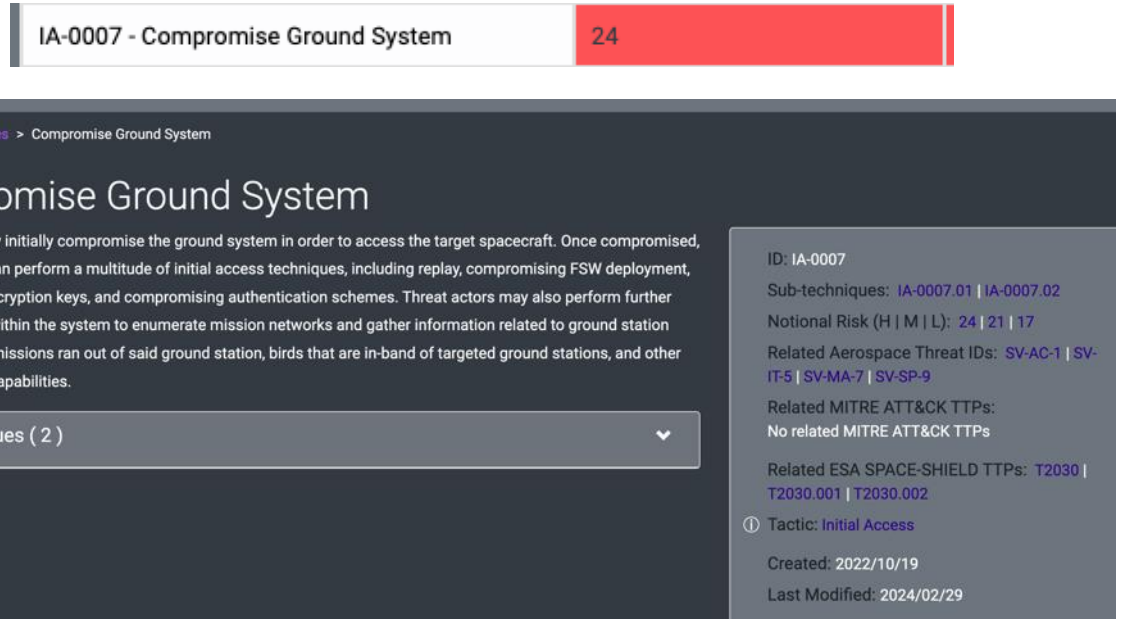




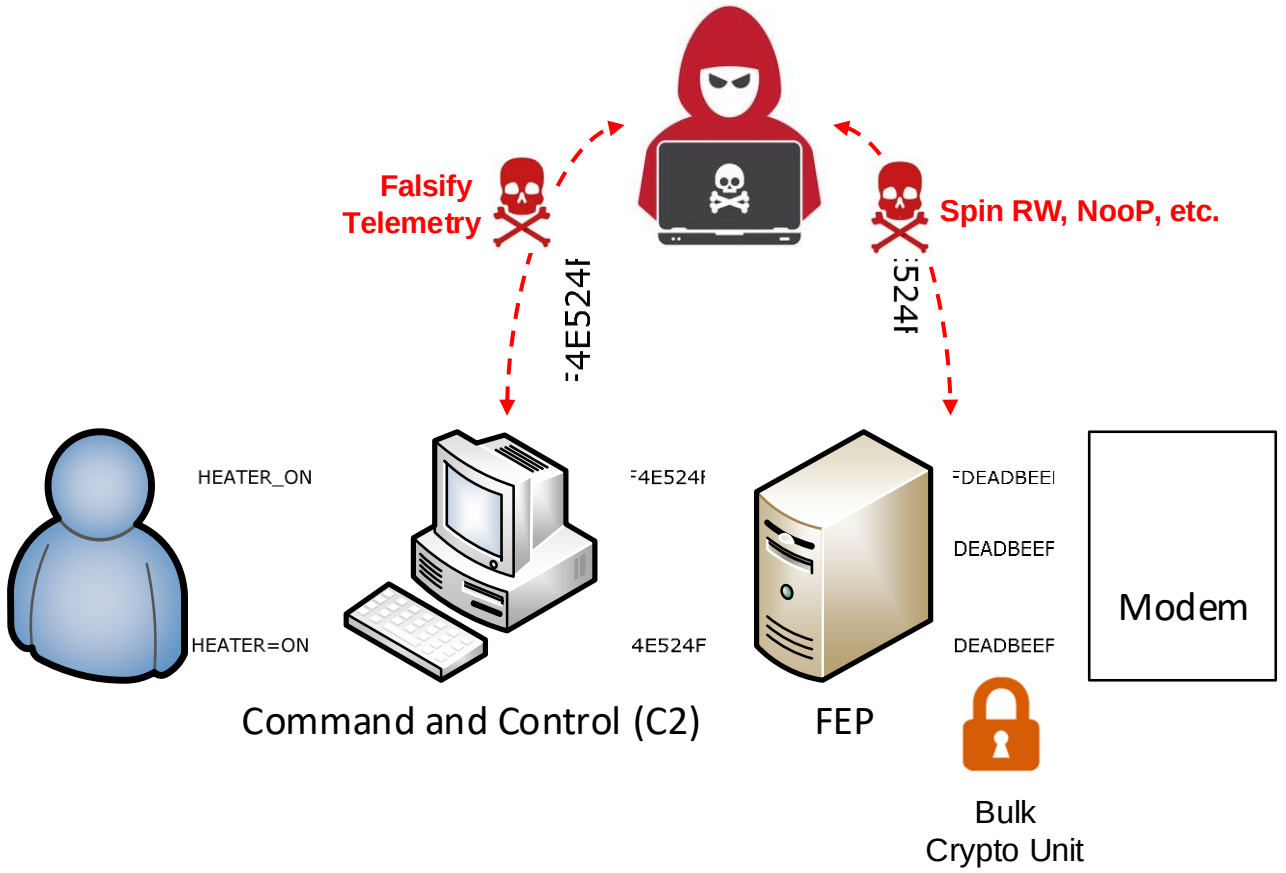
Assuming Initial Access Has Been Breached

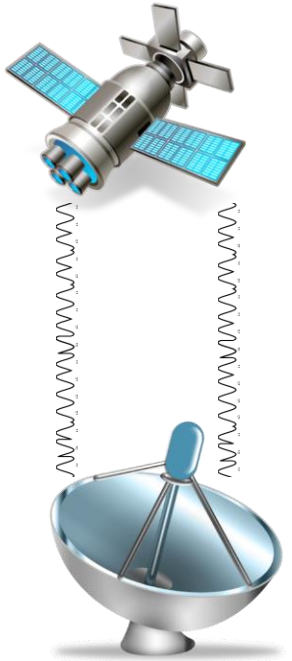
More likely than you think

- Too much focus is placed on Initial Access preventing exploits
  - “I got lots of firewalls”
  - “I’m air-gapped”
  - “I accept the risk of insider threat”
- Regardless of initial access vector, vulnerabilities can still exist!
  - Malware, poor coding in software/firmware,
    weak permissions/passwords, supply chain, insider, etc.



Performing the MitM

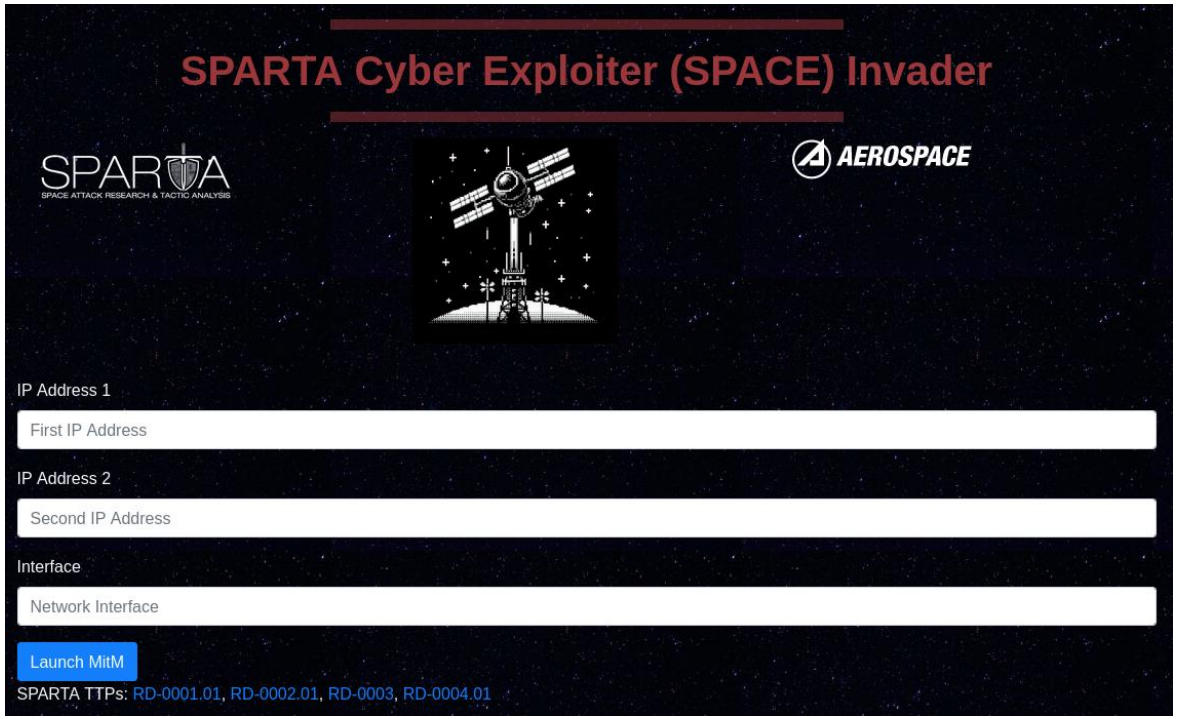


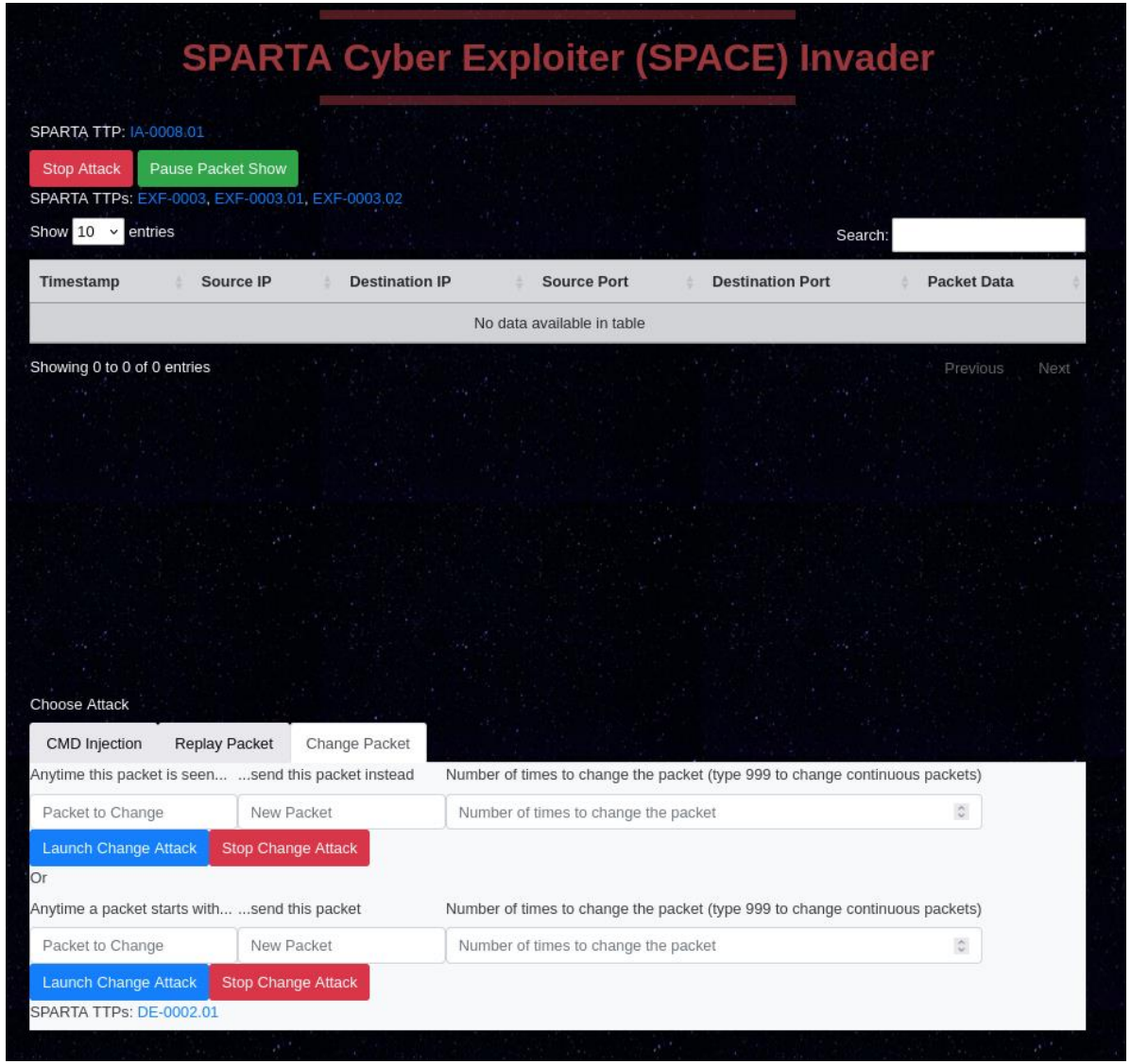


SPACE Invader

MitM Tool / Rogue Ground

- SPARTA Cyber Exploiter (SPACE) Invader
  - Acts as a rogue ground station or performs MitM attacks
  - Currently utilizes 16+ SPARTA TTPs
  - Parsers for numerous open-source ground station CMD/TLM databases

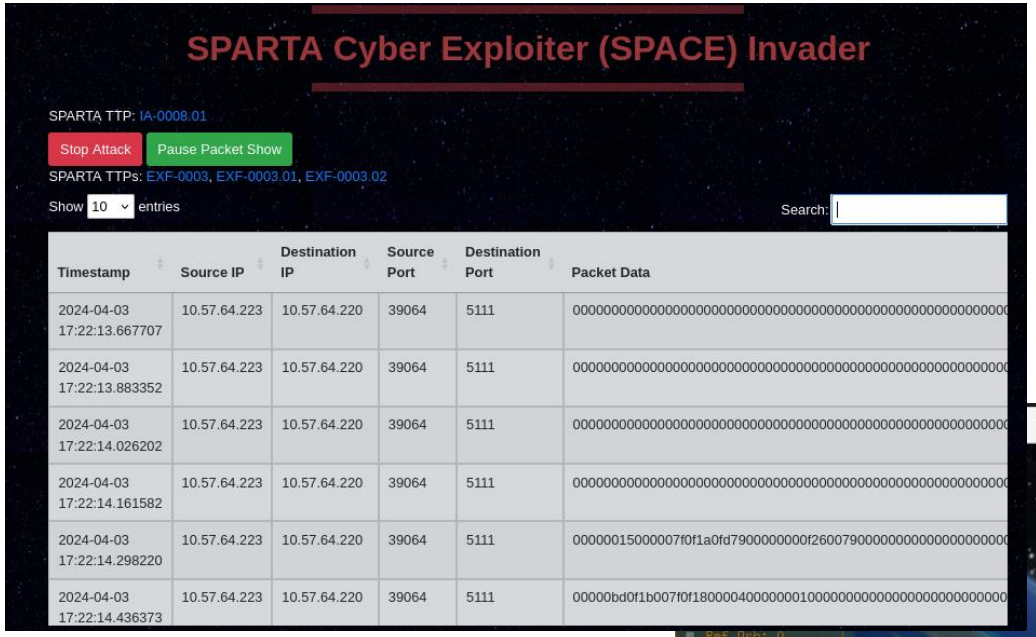


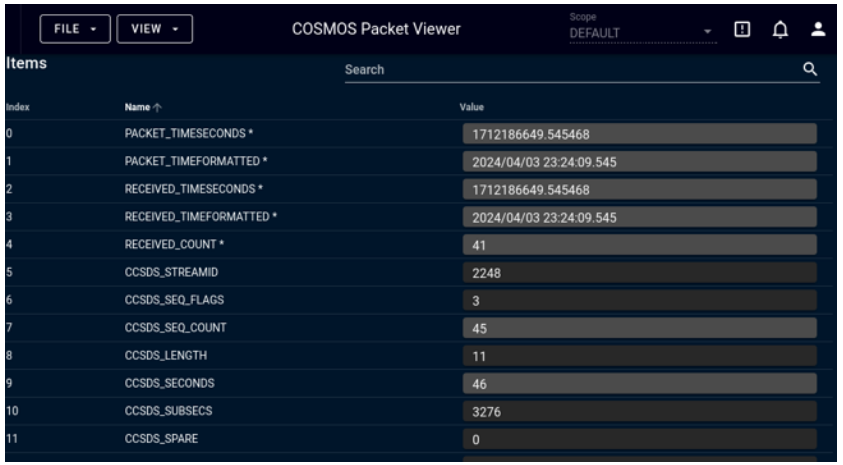


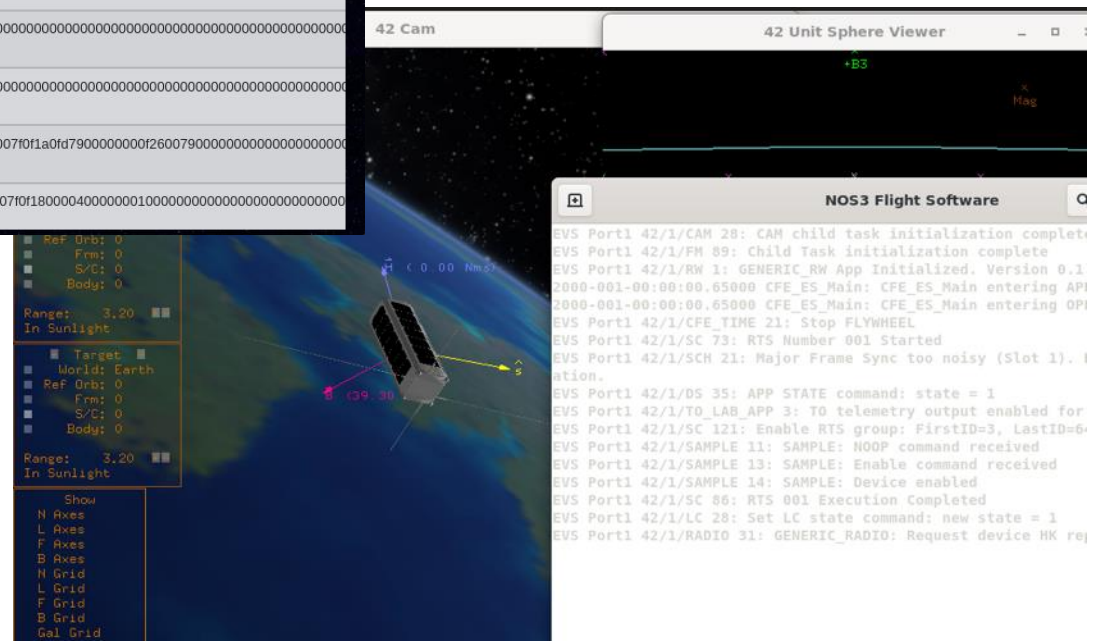
SPACE Invader (cont.)

Types 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







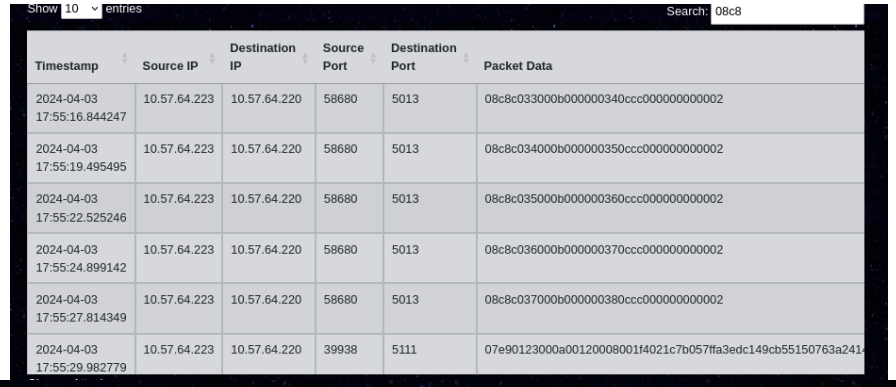
Demo Time!!!

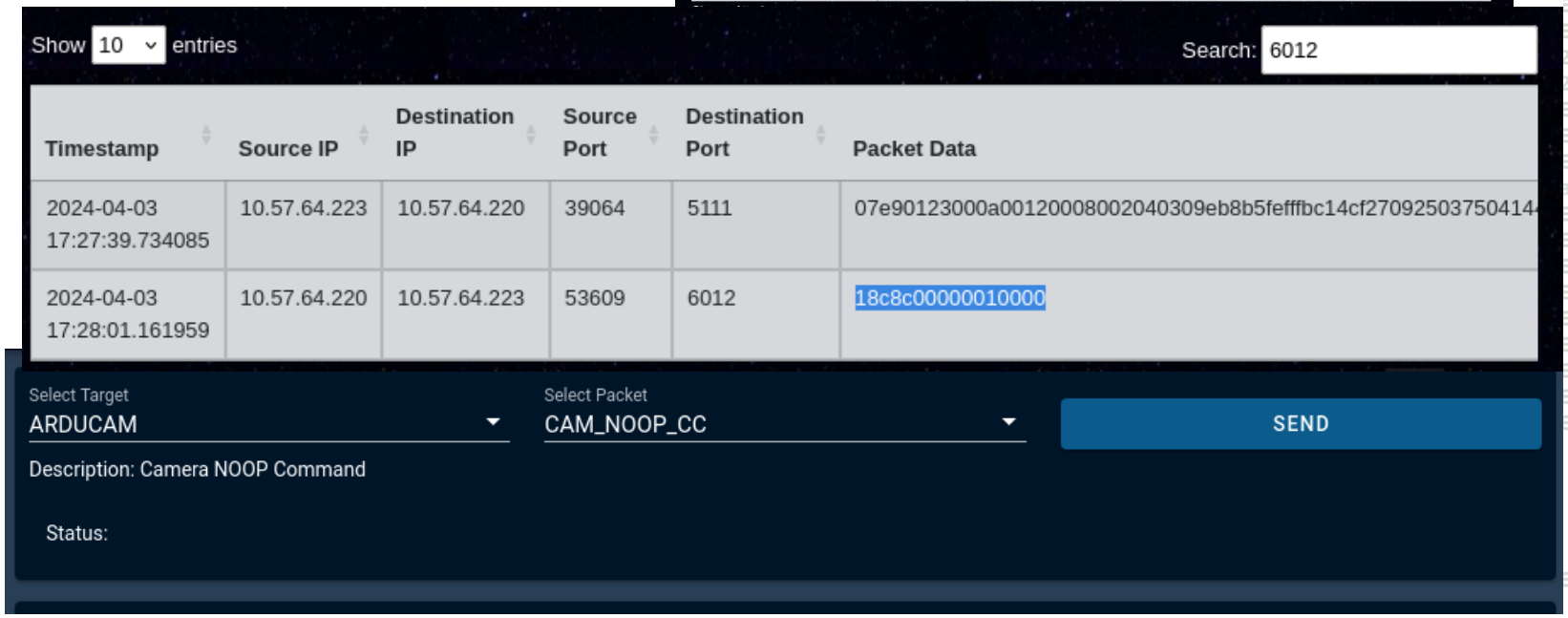
https://github.com/nasa/nos3

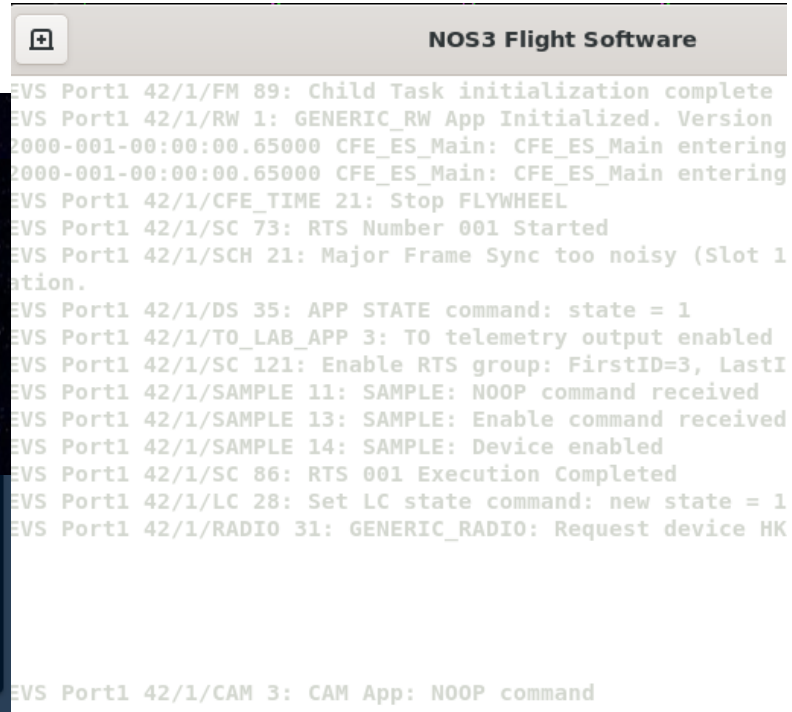
Attack #1 – Exfiltrating Telemetry and Command

You never know who's listening

- Automatically capture all telemetry and commands that are passed between the two systems
- Can use in later attacks



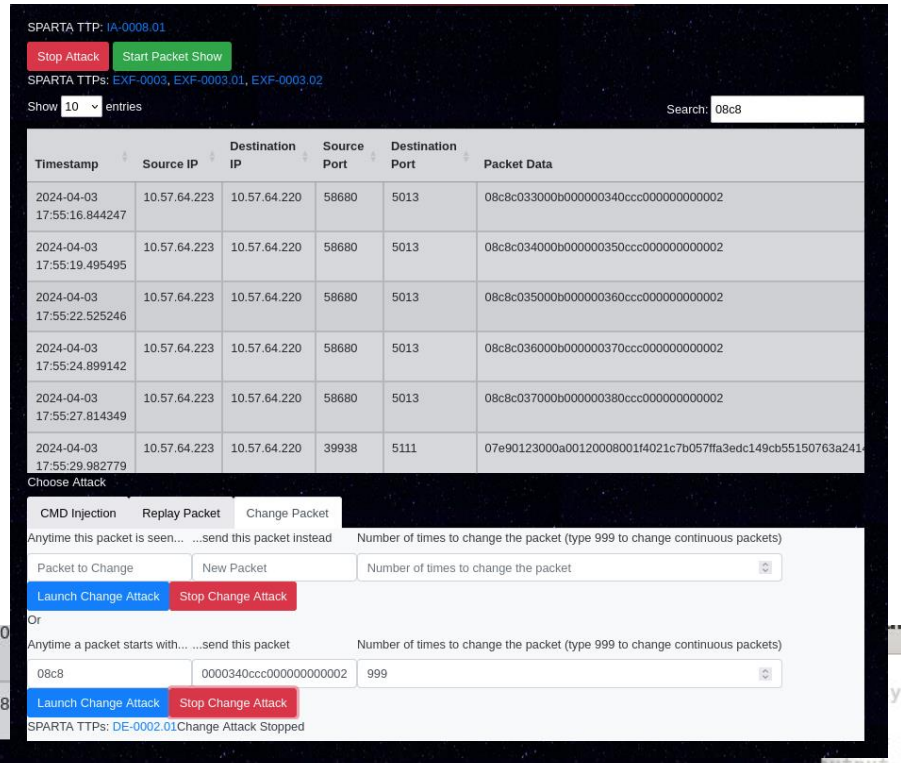


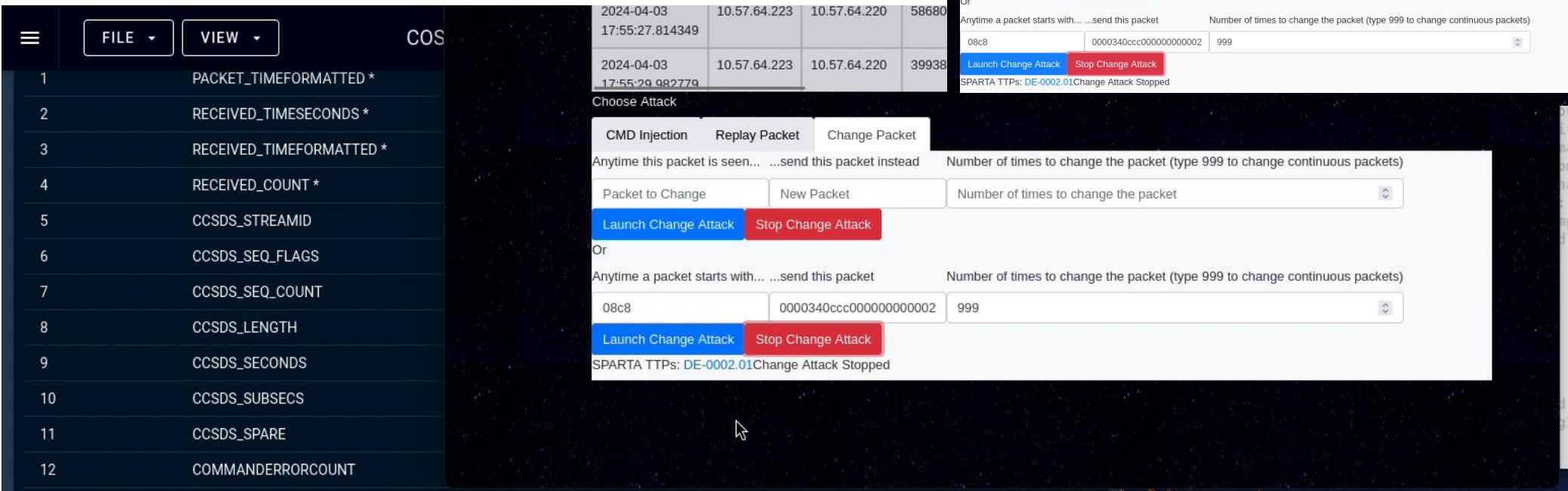


Attack #2 – Falsify Telemetry

Are you sure that's right?

- 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

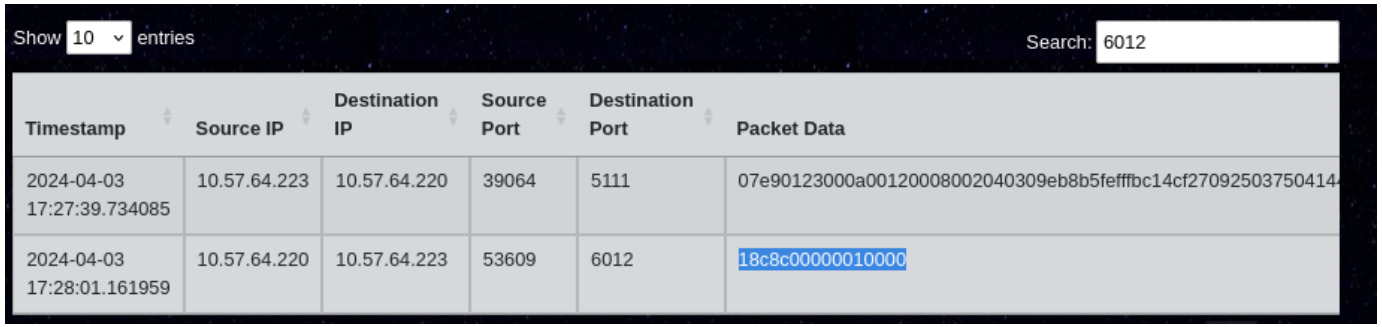


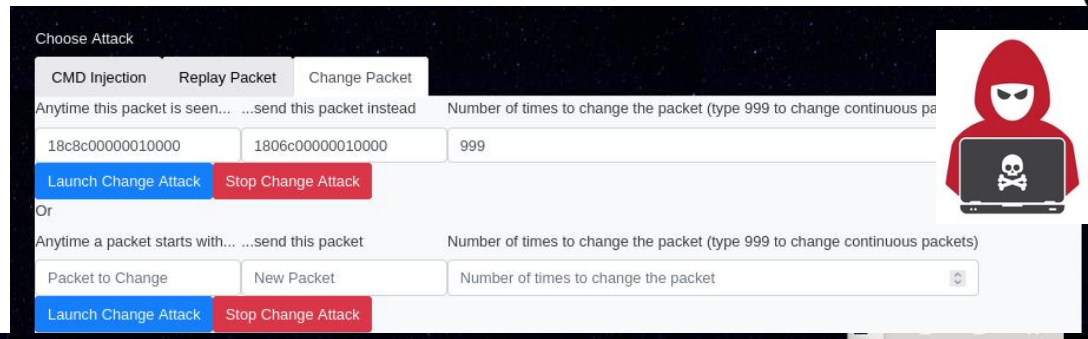


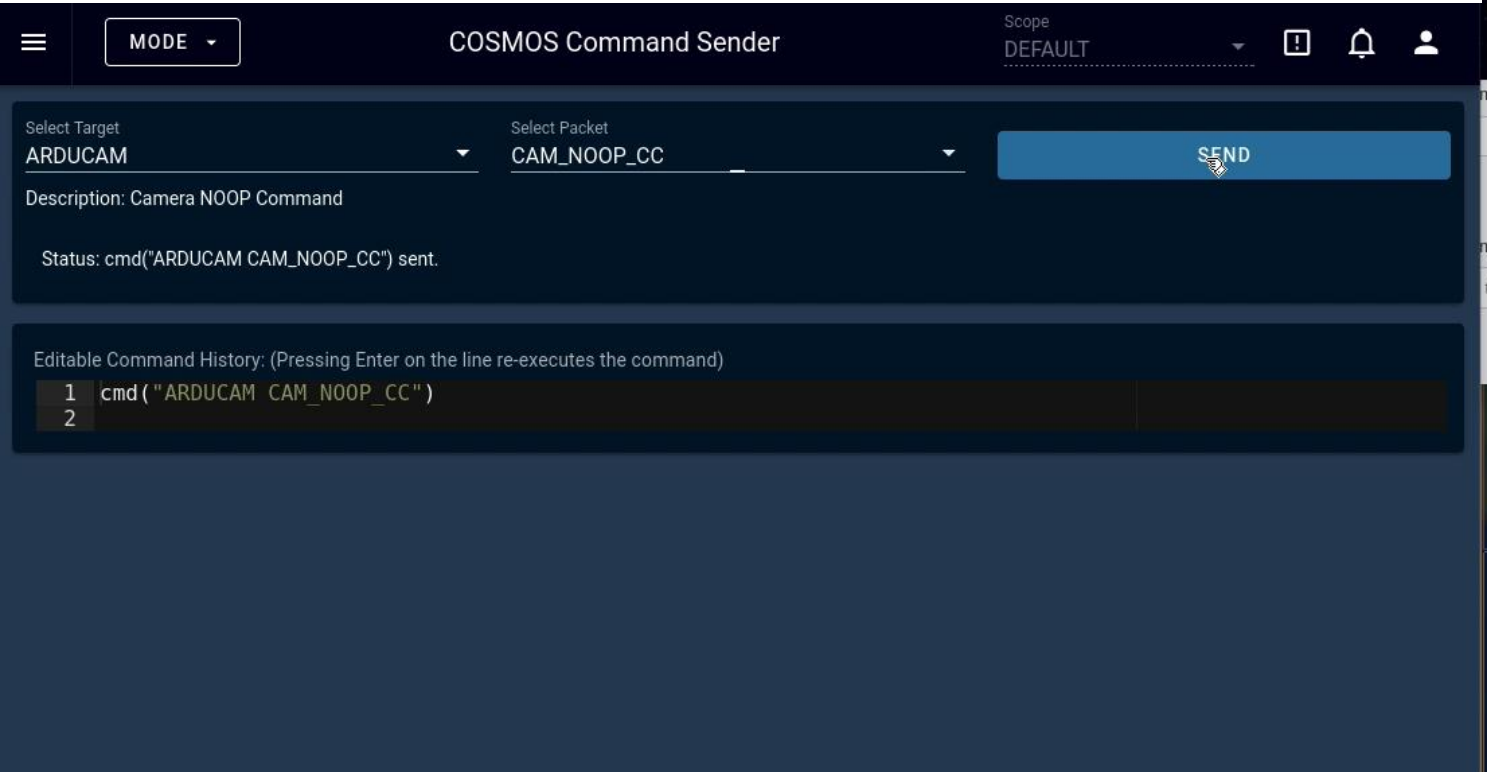
Attack #3 - Modify Packets on the Fly

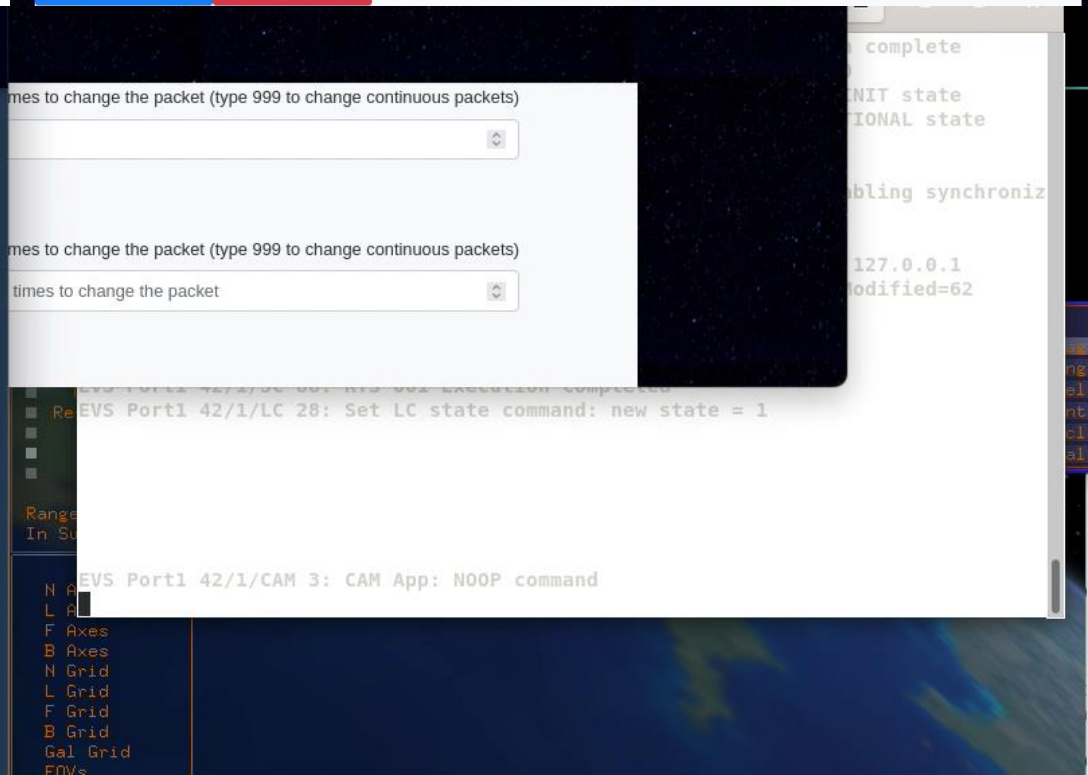
…aka the ”I don’t think so” attack

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





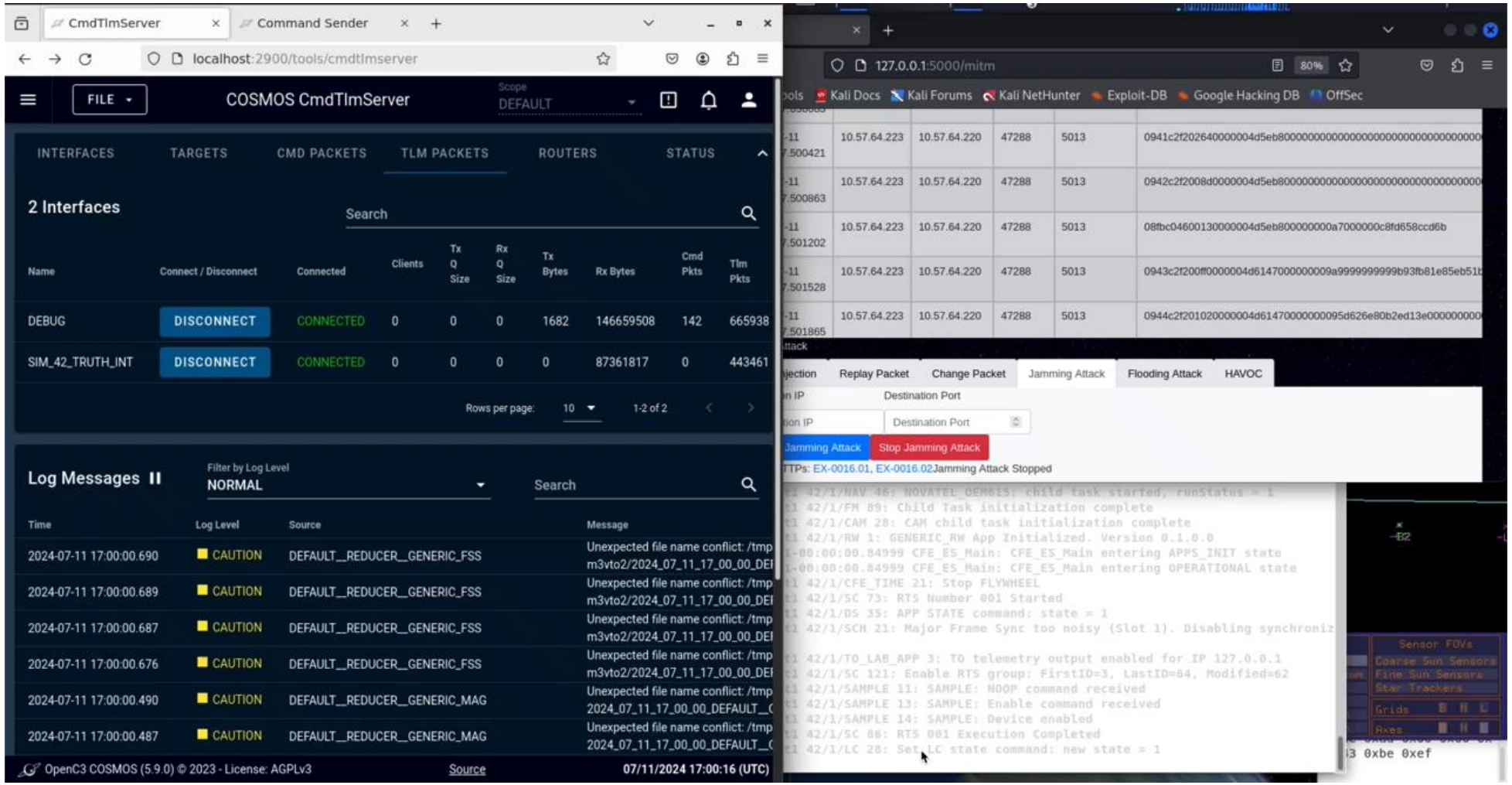




Attack #4 - Jamming

Oh no you don’t

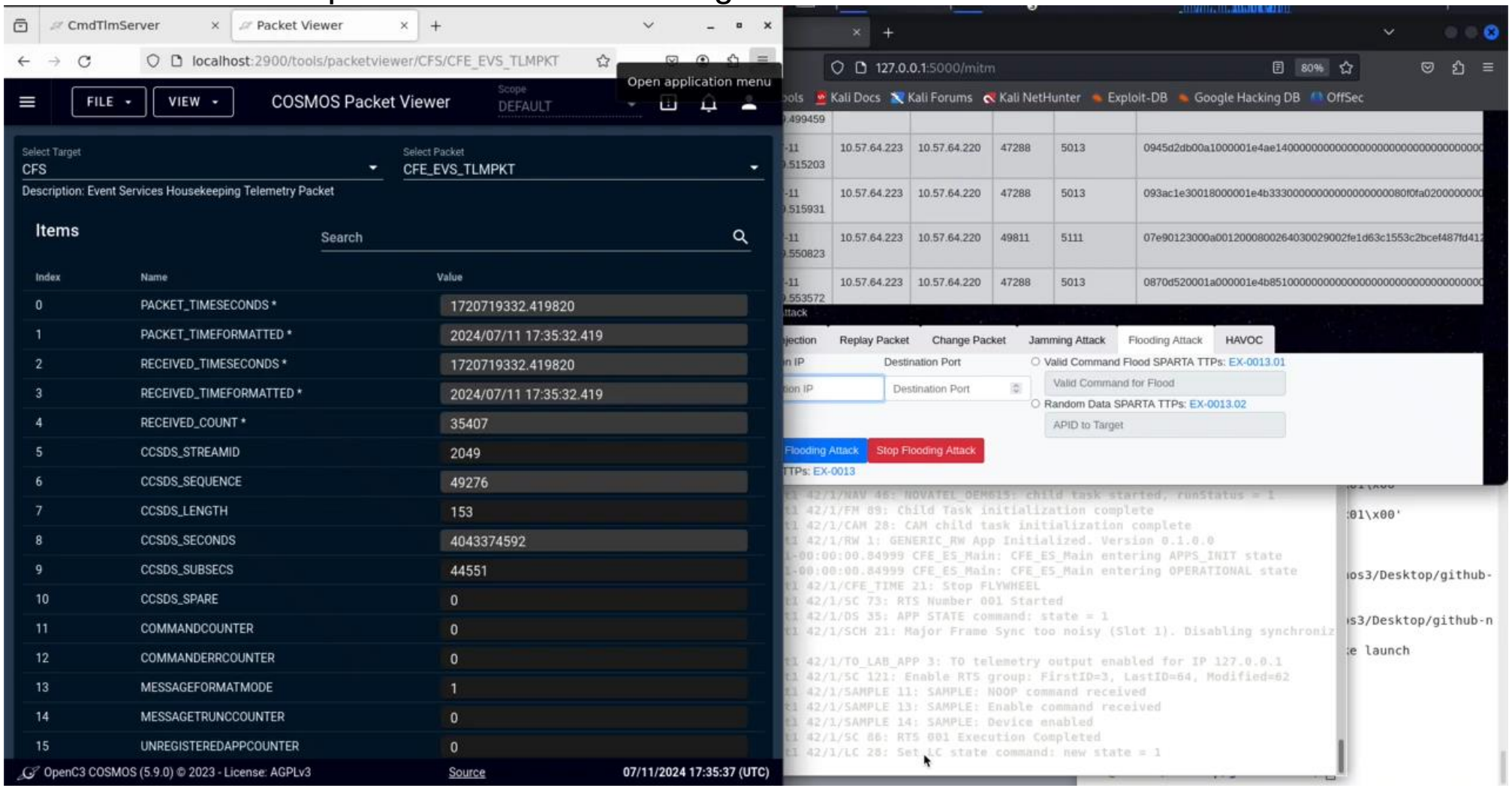
- Blocks all traffic to a specific IP and port



Attack #5 - Flooding

Mass Chaos!!

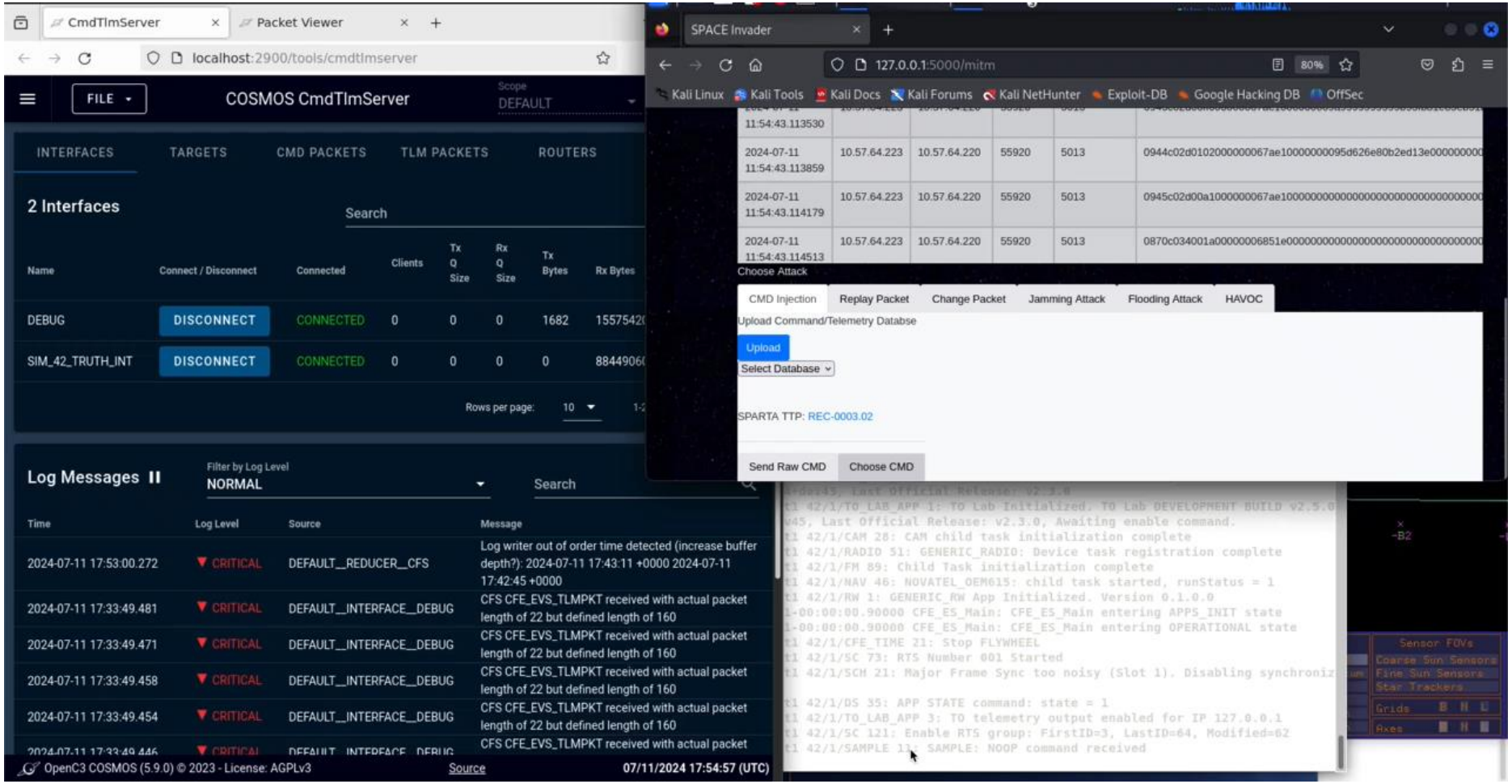
- Send random data with a specific TLM APID to the ground station



Attack #6 – Rogue Ground Station

I can do everything you can do, but better

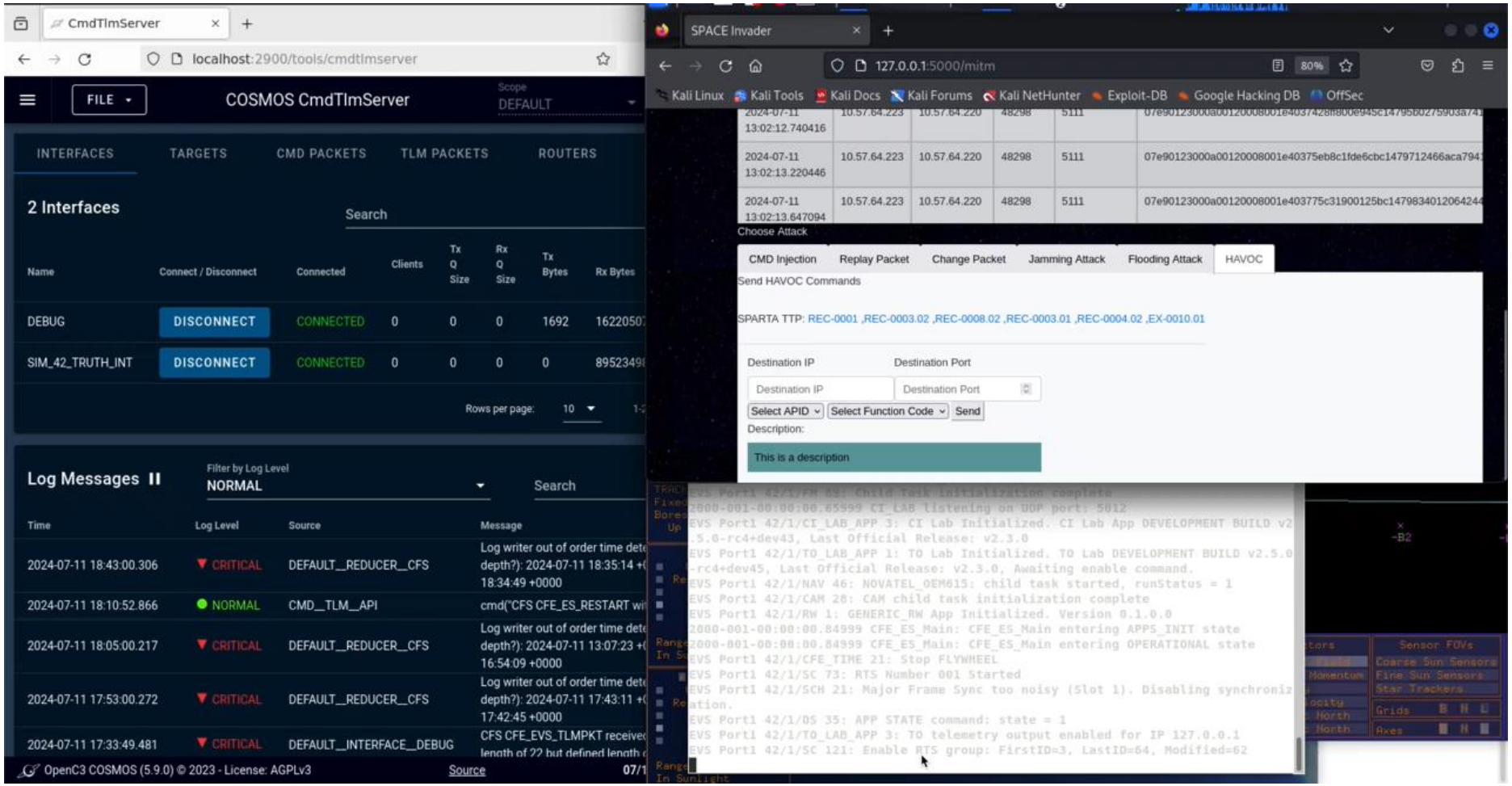
- Find the command database and load it into the tool
- Deploy commands as a normal operator



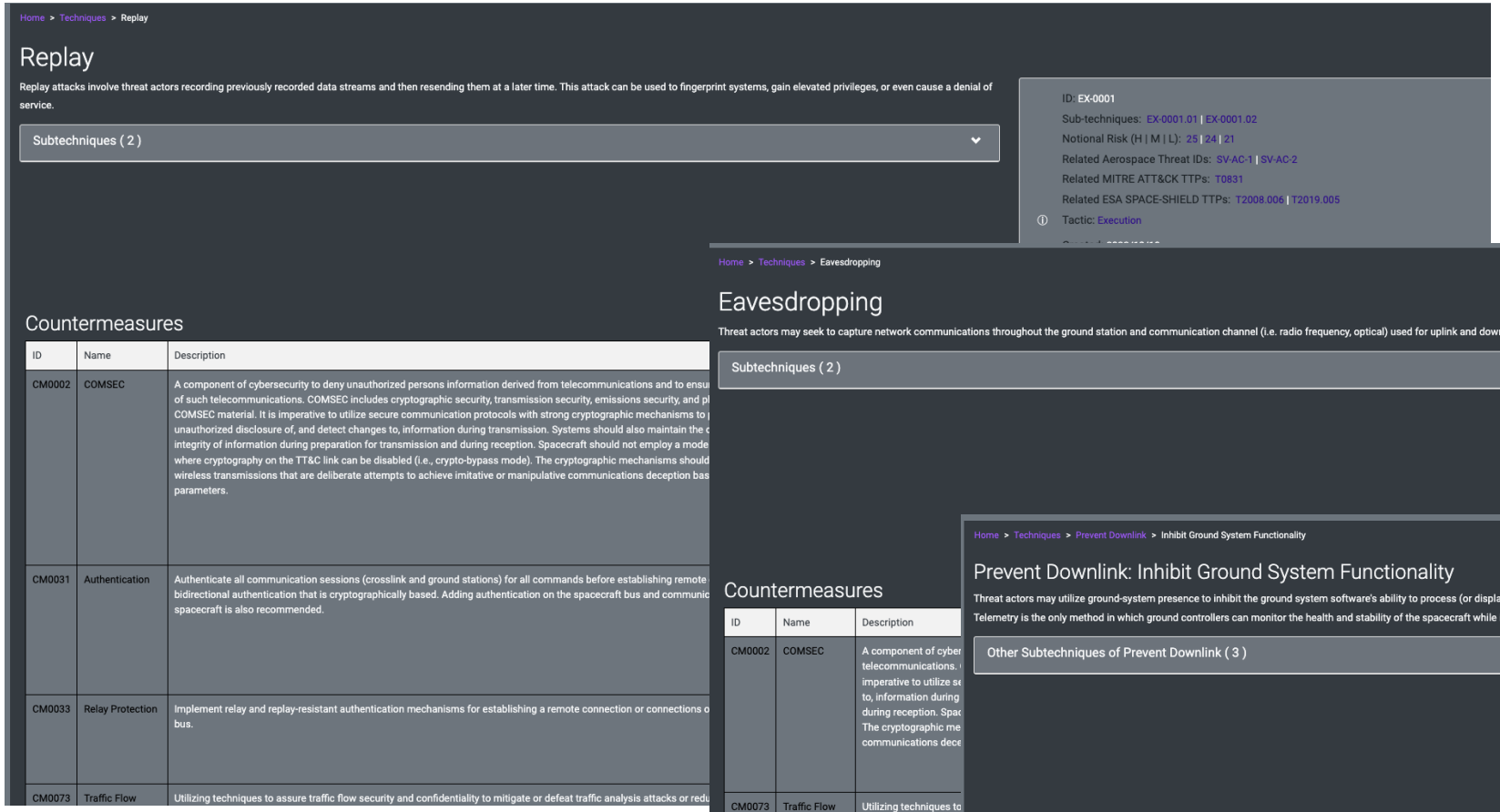
Attack #7 – Rogue Flight Application (HAVOC)

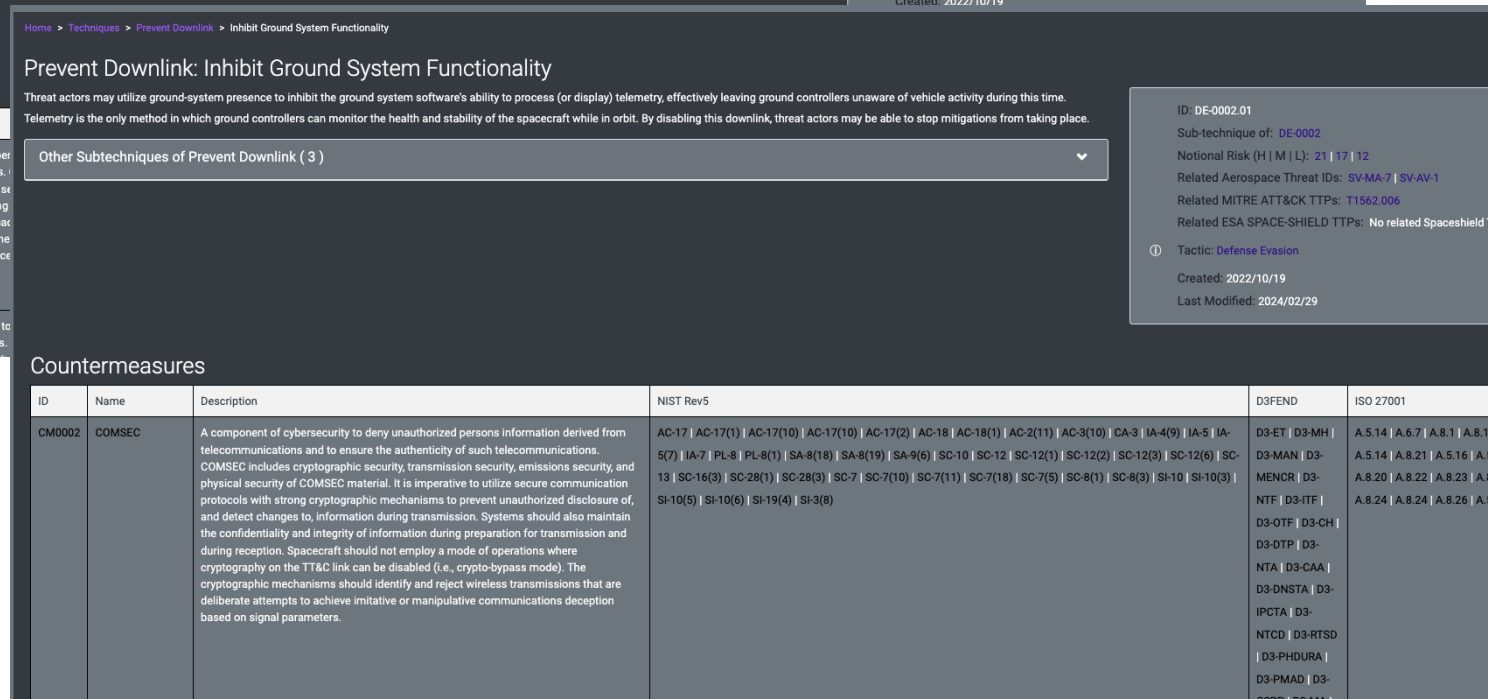
"We're in"

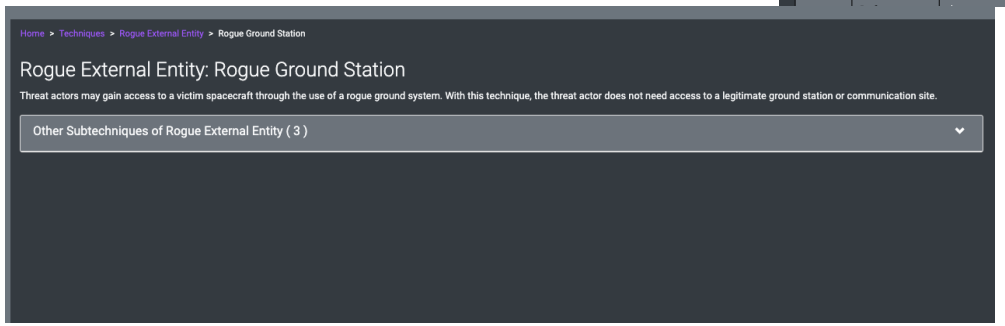
- Supply chain compromise allows for rogue flight application to be sent with the cubesat
- Can command with the rogue ground station while mission operators are unaware



Techniques Used >>> SPARTA Countermeasures





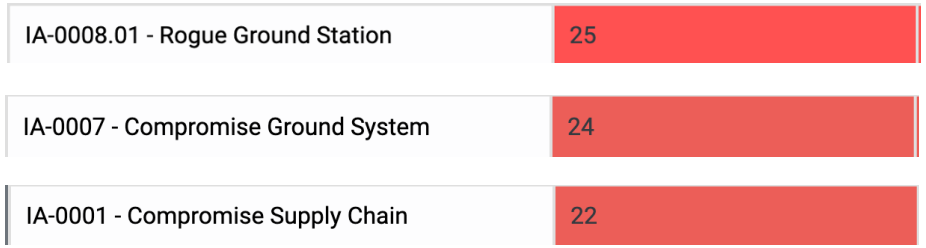


https://sparta.aerospace.org/countermeasures/SPARTA

Summary

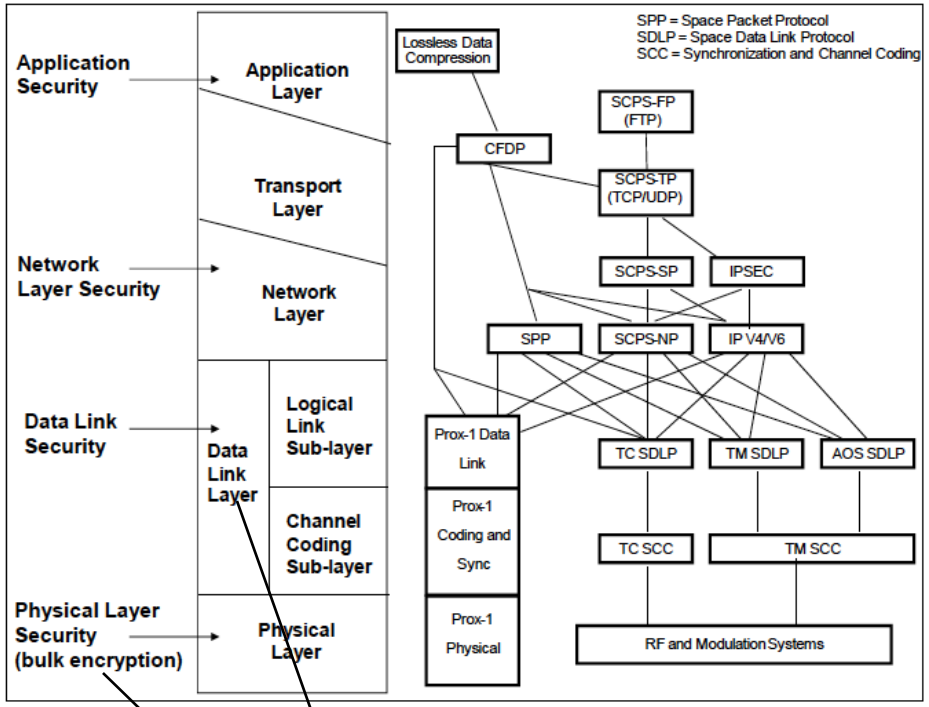
Defense in Depth is key!!!

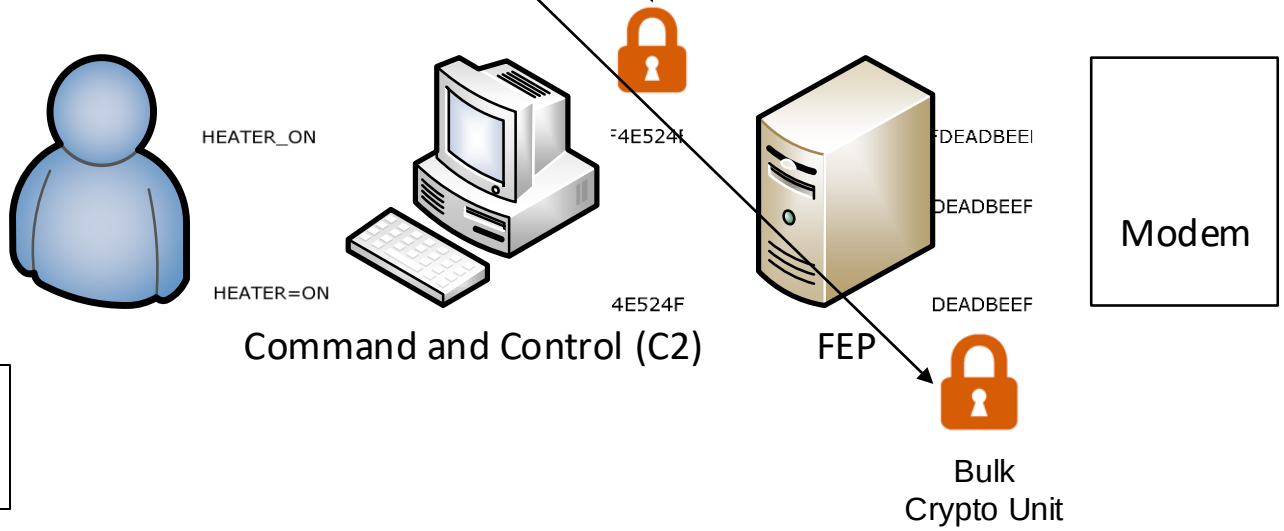
- According to SPARTA Notional Risk Scores
  - Rogue ground, compromised ground, and compromised supply chain have high risk scores to the SV

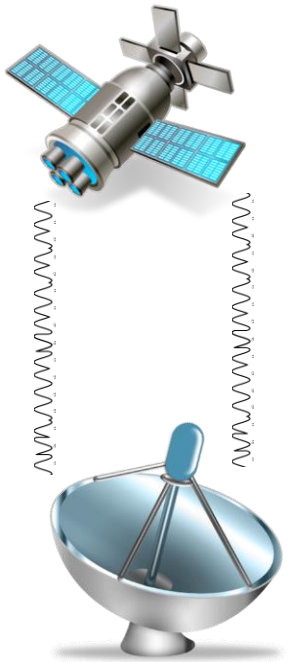


  - Add security throughout the entire mission, Not just at the end
    - Using CCSDS (TC/TM/AOS) SDLS improves security immensely and mitigates many known TTPs
      - SDLS Extended Procedures are also available

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







https://sparta.aerospace.org

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Sample Media Links:

- https://cyberscoop.com/space-satellite-cybersecurity-sparta/
- https://www.darkreading.com/ics-ot/space-race-defenses-satellite-cyberattacks
- https://thecyberwire.com/podcasts/daily-podcast/1715/notes & https://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)

Key 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

Other Papers and Resources

CYSAT '23: https://www.youtube.com/watch?v=l9nezXxO3iE
CYSAT '24: https://www.youtube.com/watch?v=jtMFl1DpAFo

- 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 TECHNOLOGY