

DEF CON Aerospace Village 2025
Hacking Space to Defend It:
Generating Indicators of Behavior
with SPARTA

# Randi Tinney, Brandon Bailey

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







brandon.bailey@aero.org & randi.j.tinney@aero.org

### Speaker Bio

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.



2019-2025

B.S. Electrical Engineering West Virginia University

Lockheed Martin Supporting National Geospatial Intelligence Agency



NASA's Independent Verification and Validation Program

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

Transitioned to NASA Government Employee GS-13

Began "Hacking" Space Systems

2013

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

2019

2013-2024

2018

Left the Government as GS-15 to become

Chief Technology Officer (CTO) for small

- Supported NASA part-time as contractor

business in West Virginia

AEROSPACE





DefCON 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

• Example Papers/Articles:

2019: <u>Defending Spacecraft in the Cyber Domain</u>

- 2020: Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices

2021: Cybersecurity Protections for Spacecraft: A Threat Based Approach

2022: <u>Protecting Space Systems from Cyber Attack</u>

2024: Space Segment Cybersecurity Profile

July 2022 Congressional Testimony:

Video: <a href="https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964">https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964</a>

Written Testimony: <a href="https://republicans-science.house.gov/\_cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf">https://republicans-science.house.gov/\_cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf</a>

SPARTA Launched

https://sparta.aerospace.org





- 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)
- Space Network Ground Segment Sustainment (SGSS)
- 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



2

#### 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 <u>MITRE ATT&CK</u>) 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 threat-informed information to space professionals about how spacecraft may be compromised

#### Intel or Attacker Driven Countermeasure / Control / Requirement Derivation







SPARTA Techniques

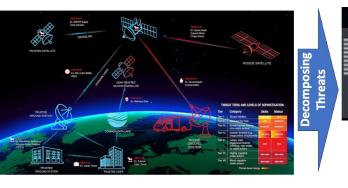


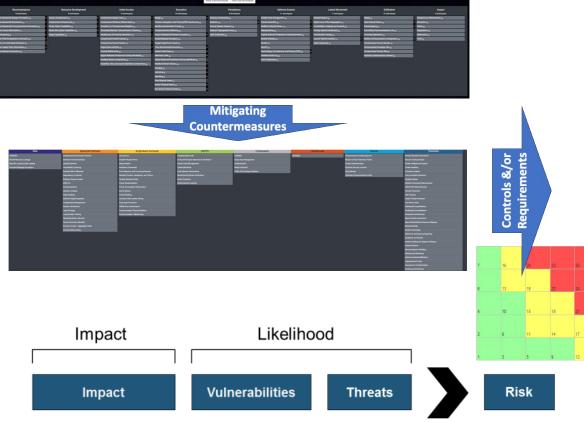
Space Attack Research & Tactic Analysis (SPARTA)

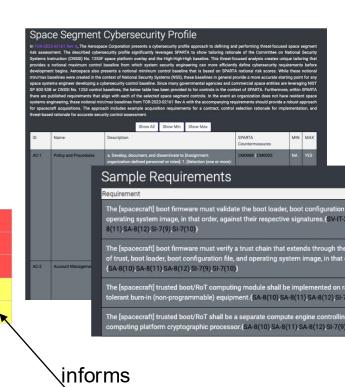
SPARTA Countermeasures



NIST SP 800-53 Controls



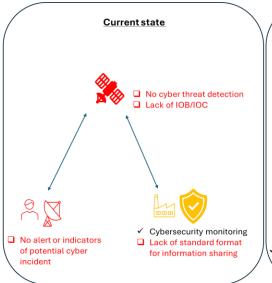


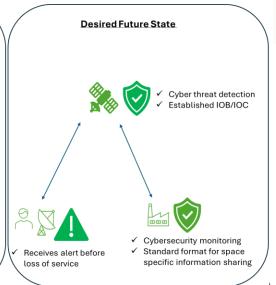


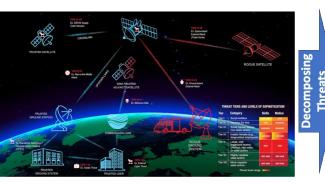
https://sparta.aerospace.org/notional-risk-scores

#### Similar Process Applies for IOBs/Detection Engineering

Translating Techniques to Detections













Inform Ground

### SPARTA Indicators of Behavior (IOBs) – Launched April 2025



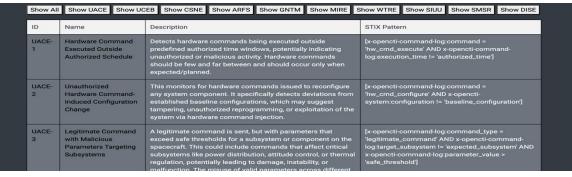
A crucial element in modern spacecraft defense

- Funded by the <u>Department of Homeland Security (DHS) Science and Technology (S&T) Directorate</u> to enhance the cybersecurity posture of space systems, addressing the growing need for proactive threat detection as space infrastructure becomes increasingly critical to national security and economic stability
  - BLOG: <a href="https://medium.com/the-aerospace-corporation/indicators-of-behavior-iobs-in-sparta-v3-0-c42ab0683100">https://medium.com/the-aerospace-corporation/indicators-of-behavior-iobs-in-sparta-v3-0-c42ab0683100</a>
- Designed to identify behavioral patterns that could indicate emerging threats versus Indicators of Compromise (IOCs) which
  focus on detecting known malicious artifacts or signatures
  - IOCs are evidence of KNOWN threats (i.e., for incident response, forensics) where IOBs are patterns of suspicious or malicious behavior (i.e., for threat hunting, proactive monitoring.)
    - IOCs would imply you already know and have these same components and aspects, etc. because IOCs operate in a deterministic, direct-detection paradigm, where known observables match against system telemetry.

• IOBs operate in a probabilistic, behavior-based paradigm, where higher-level abstractions are mapped to system specifics through

translation, enabling detection of unknown or evolving threats.

https://sparta.aerospace.org/related-work/iob



 Allows space system developers to build detection mechanisms for anomalies and suspicious activities onboard the spacecraft

In this first iteration, ~200 IOBs were created

#### **Generating SPARTA's Initial IOBs**

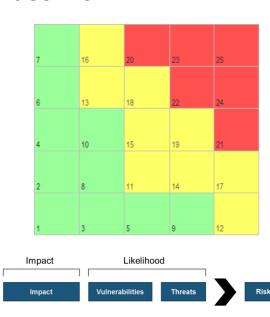
#### Red informing Blue

- Turning theory into detection: we didn't just theorize, we attacked
  - We applied real SPARTA techniques against flight-like systems to observe what adversary behavior actually looks like on a spacecraft.
- From red team to real defenses, offensive testing revealed how attacks manifest in data which informs the design of IOBs tailored to actual spacecraft subsystems
- SPARTA gave us the threats/techniques
  - Risk-ranked techniques (NRS <a href="https://sparta.aerospace.org/notional-risk-scores">https://sparta.aerospace.org/notional-risk-scores</a>)
     helped us prioritize behaviors that could detect high impact and high likelihood techniques
- Instead of relying on static IOCs, we crafted behavioral detections for unauthorized commands, memory tampering, signal manipulation, and more
- Fusing subsystem telemetry, logs, and command histories, we translated generic IOB patterns into mission-specific observables.
- Every IOB will need engineering translation, but the STIX patterns are a starting point
- We validated each IOB in realistic environments
  - Using cyber ranges, FlatSats, and digital twins, we tested detections across normal and adversarial conditions to refine fidelity and reduce false positives.

**Behavior Over Signatures: Building Real Cyber Detections for Spacecraft** 

# Top 50 NRS scored techniques leveraged for initial SPARTA IOB Baseline

SPARTA Techniques/Sub-Techniques	Notional Risk (HIGH Criticality Systems)			
IA-0004 - Secondary/Backup Communication Channel	25			
IA-0004.01 - Ground Station	25			
IA-0007.02 - Malicious Commanding via Valid GS	25			
IA-0008 - Rogue External Entity	25			
IA-0008.01 - Rogue Ground Station	25			
EX-0001 - Replay	25			
EX-0001.01 - Command Packets	25			
EX-0005 - Exploit Hardware/Firmware Corruption	25			
EX-0005.02 - Malicious Use of Hardware Commands	25			
EX-0009.01 - Flight Software	25			
EX-0009.03 - Known Vulnerability (COTS/FOSS)	25			
EX-0013 - Flooding	25			
EX-0013.01 - Valid Commands	25			
EX-0013.02 - Erroneous Input	25			
EX-0014 - Spoofing	25			
EX-0014.01 - Time Spoof	25			
EX-0014.02 - Bus Traffic Spoofing	25			
EX-0014.04 - Position, Navigation, and Timing (PNT) Spoofing	25			
EX-0016.03 - Position, Navigation, and Timing (PNT) Jamming	25			
PER-0003 - Ground System Presence	25			
DE-0002.02 - Jam Link Signal	25			
EXF-0007 - Compromised Ground System	25			



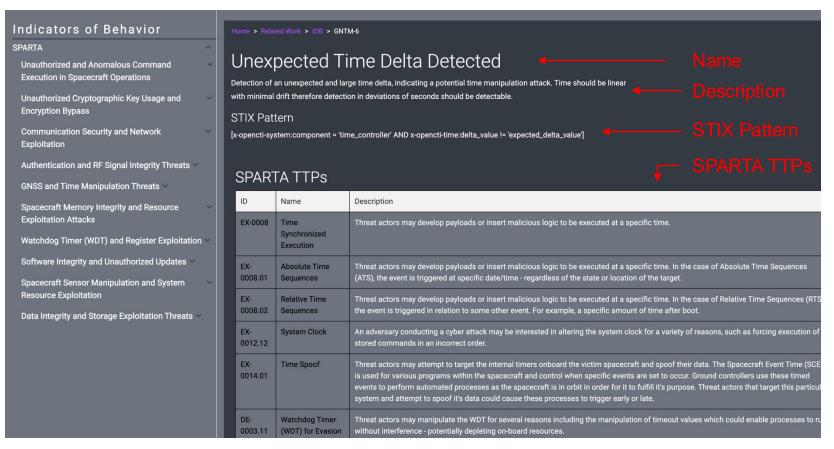
#### **SPARTA's IOB Behavioral Categories**

- ~200 IOBs Fall into 10 Categories
  - IOBs are currently organized within SPARTA into 10 distinct categories, where each IOB has their own unique identifiers.
    - UACE Unauthorized and Anomalous Command Execution
      - Detects out-of-profile or malicious command activity, including replays, flooding, or safe-mode abuse, that could jeopardize spacecraft control.
    - UCEB Unauthorized Cryptographic Key Usage and Encryption Bypass
      - Flags suspicious crypto key usage and encryption changes that may indicate attempts to bypass secure communications or gain persistent access.
    - CSNE Communication Security and Network Exploitation
      - Monitors network traffic and protocol anomalies to detect rogue access, data interception, or denial-of-service targeting communication links.
    - ARFS Authentication and RF Signal Integrity Threats
      - Identifies authentication failures, RF anomalies, or signal spoofing that may signal adversary attempts to impersonate or disrupt control channels.
    - GNTM GNSS and Time Manipulation Threats
      - Detects GNSS jamming, spoofing, or time desynchronization attempts that threaten navigation accuracy and mission synchronization.
    - MIRE Spacecraft Memory Integrity and Resource Exploitation
      - Monitors for memory corruption, unauthorized access, or resource exhaustion that could degrade performance or introduce malicious code.
    - WTRE Watchdogs and Register Exploitation
      - Detects tampering with watchdog timers or critical registers that adversaries may target to disable failsafes or destabilize spacecraft systems.
    - SIUU Software Integrity and Unauthorized Updates
      - Tracks unauthorized flight software changes, unvalidated updates, or firmware tampering that may introduce backdoors or disrupt operations.
    - SMSR Sensor Manipulation and System Resource Exploitation
      - Detects spoofed sensor data or abnormal resource usage that could mislead spacecraft logic or degrade key system functionality.
    - DISE Data Integrity and Storage Exploitation
      - Monitors file systems and storage for corruption, unauthorized deletions, or data manipulation that threaten mission data and continuity.

#### **Using SPARTA IOB for IDS Creation**

Unexpected Time Delta Detected Example

- SPARTA provides a lot of information about the IOB for any would-be developer to get started
  - STIX pattern shows key information for how IOB is generated and what values should be equal to
- Shows the various SPARTA TTPs that this IOB could be indicating on
  - Just because one IOB may be triggered, does not mean that the SPARTA TTP is being performed. Each SPARTA TTP has multiple IOBs that could indicate they are being done



Can developer who did not create the IOBs interpret and develop detection on a spacecraft?

#### **IDS Experiment Setup**

Initial Proof of Concept – Testing the Theory

- Utilizing NASA's NOS3 open-source and free digital twin
  - cFS utilized for spacecraft software (Coded in C)
  - COSMOS utilized for ground station (Coded in Ruby)
- IDS (SpaceCOP) migrated to a cFS application that runs on-board the spacecraft within the FSW
  - Features ~30 different SPARTA IOB detections
  - Created custom kernel module to monitor for SYSCALLs
  - Monitors file integrity
  - Monitors disk/memory/CPU utilization
  - Hooks into the software bus to monitors sensor states and commands
  - Monitors for time delta
- The added IDS does not overwhelm system resources, showing that it is an effective way to monitor for IOBs
   Without SpaceCOP Running

PID	USER	PR	NI	VIRT	RES	SHR S	%CPU	%MEM	TIME+ COMMAND	
8169	root	rt	0	1109212	24636	19644 S	6.3	0.2	0:02.71 core-cpu1	
With SpaceCOP Running										
PID U	JSER	PR	NI	VIRT	RES	SHR S	%CPU	%MEM	TIME+ COMMAND	
3265 r	oot	rt	0	1167696	27280	21776 S	7.3	0.2	3:12.10 core-cpu1	





### **IDS Experiment Setup (cont.)**

Unexpected Time Delta Detected IOB Example

- Unexpected Time Delta IDS detection code within SpaceCOP
- Define TIME\_THRESHOLD

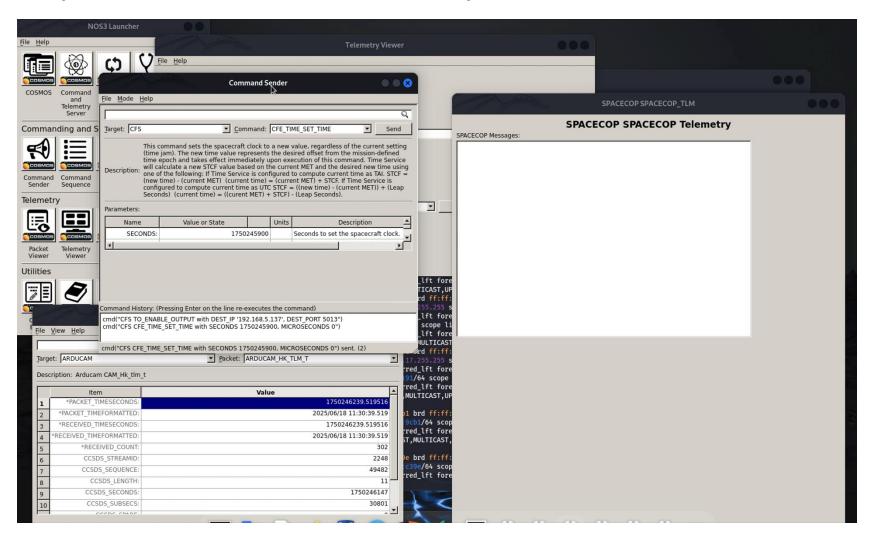
[x-opencti-system:component = 'time\_controller' AND x-opencti-time:delta\_value != 'expected\_delta\_value']

- Initializes at 5 seconds but can be changed via command sent from ground station later
- Gets time via cFS API call (CFE\_TIME\_GetTime)
- If system is first starting up, store the seconds in "expected\_time" value
- Else, see if the current seconds +/- defined TIME\_THRESHOLD is larger than the "expected\_time"
- If so, report the time delta is unexpected
- Store the current seconds for next iteration

```
#define TIME THRESHOLD 5
void check time()
    CFE TIME SysTime t time = CFE TIME GetTime();
    char message[IDS REPORT MESSAGE LEN];
    uint32 packet time;
    uint32 delta;
    if(startup)
        expected time = time.Seconds;
        printf("[SPACECOP] - Initial timestamp %d detected\n", expected time);
        SPACECOP SetStartup(0);
        packet time = time.Seconds;
         f(expected time < packet time-TIME THRESHOLD || expected time > packet time+TIME THRESHOLD).
            delta = expected time - packet time;
            printf("[SPACECOP] - Time Delta is %d which is greater than threshold %d\n", delta, TIME THRESHOLD);
            memset(message, 0, sizeof(char) * IDS REPORT MESSAGE LEN);
            snprintf(message, IDS REPORT MESSAGE LEN, "[SPACECOP] - Time Delta is greater than threshold %d\n", TIME THRESHOLD);
            SPACECOP ReportIDSMsg(message);
        expected time = packet time;
```

### **Testing the Detection**

#### Unexpected Time Delta Detected Example



[SPARTA TTP (e.g., EX-0014.01)]

↓ (used in red team exploitation)

[Real Attack Observed]

[Behavior Modeled as IOB]

↓ (engineered detection logic)

[STIX Pattern Created]

↓ (IDS Rule Implemented)

[Detection Validated in FlatSat]



#### **Experiment Worked Once...**

Do the IOBs Scale?

- After applying on a small subset of IOBs successfully, we asked:
   Does this scale? Can all SPARTA IOBs translate into real, mission-specific data?
- The challenge
  - SPARTA IOBs are designed to be generic, but can they be mapped to actual telemetry, command logs, and onboard activity?
- We know translation is needed
  - Mapping STIX-based IOBs to spacecraft-specific data (e.g., telemetry mnemonics, onboard processes, message formats) is required
- Key Questions to Answer
  - Are IOBs specific enough to anchor real detection logic?
  - Can we consistently map IOB observables (e.g., STIX patterns) to existing spacecraft data fields?
  - What translation or engineering lift is needed?
- Approach: Initiated a full mapping effort where we translated IOBs into spacecraft-specific telemetry
  - Bonus Concept: Can this be automated?







#### STIX Matcher: Automating for Detection and Reporting System (DARS)

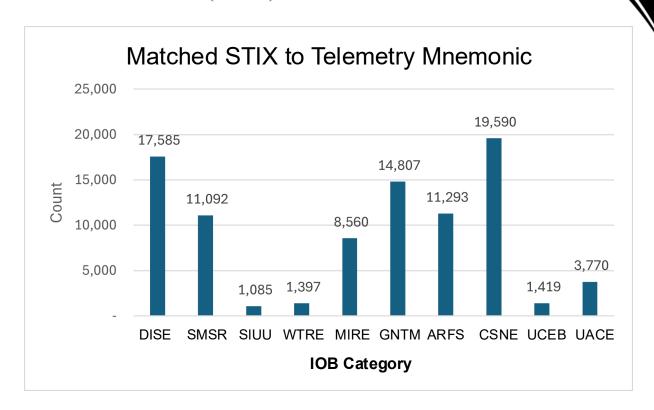
Correlating satellite hardware metrics with Indicators of Behavior (IoBs)

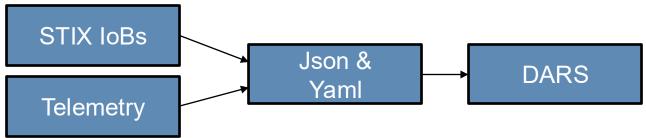
#### Matching Telemetry Master list to STIX SPARTA loBs

- From a master list of 436,230 satellite telemetry mnemonics identified 92,450 unique Telemetry Mnemonics with 90,598 matches to STIX.
- Built a modular, batch cached, parallelized, semantic matching Neuro linguistic programming (NLP) pipeline that is reusable for other telemetry or STIX datasets.

#### Automatically Generating Rules for Intrusion Detection with DARS

- Only a small subset of the master Telemetry Mnemonics are used by any individual satellite.
- Automates the matching of mnemonics between the main list and any individual satellite.
- Then generates rules in Json format to be read by DARS for intrusion detection.





Automatically matches the 92,450 unique Telemetry Mnemonics with SPARTA's initial set of IOBs

### **Beyond Theory: Testing IOBs Against Advanced Threats**

Detecting Actual Malware and Advanced Persistent Threats Onboard

- Validated that STIX-based IOBs can be mapped to mission-specific telemetry
  - But telemetry matching alone doesn't confirm effectiveness.
    - Mapping alone doesn't prove detection works when it counts
- Next question
  - Can IOBs catch stealthy threats like embedded malware, rogue apps, or compromised boot code?
- Introducing advanced threats into flight-like environments like supply chain malware, rogue flight apps, and more
  - → to stress-test the IOB framework under operationally realistic conditions



### **Expanding SpaceCOP to Detect IOBs for Malware?**

Introducing Blackout

- Blackout is a rogue cFS application that
  - Allows the threat actor full root access to the operating system
- Malicious Code (4)

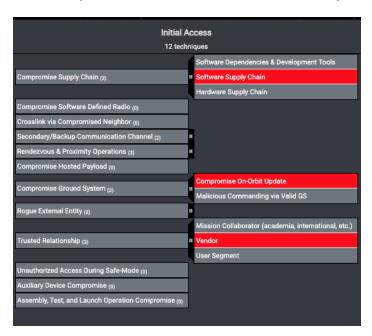
  Malicious Code (4)

  Rootkit

  Bootkit

https://sparta.aerospace.org/technique/EX-0010/

- Provides a "shell-like" interface
  - Similar to a Command and Control (C2) server for space systems
- Can upload/download files to the spacecraft
  - Very similar to NASA's CFDP, but does not depend on any prior installs of the system
- Initial Access is Supply Chain Attack
  - This malware could also be loaded on the system in some capacity through a malicious update
- Malware could be automatic, or it could need interaction from ground (real or rogue)

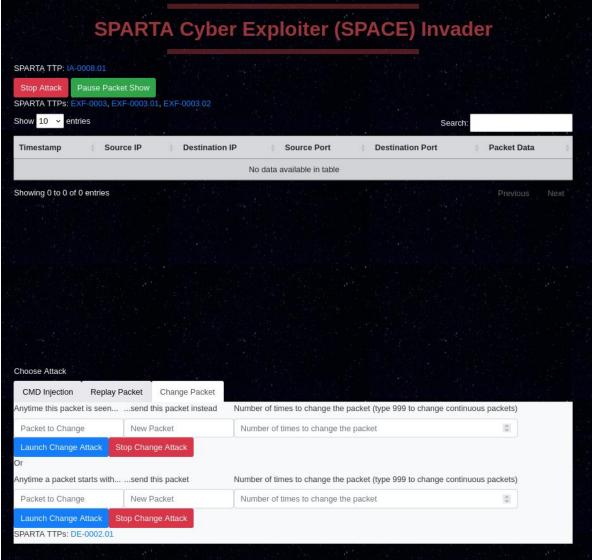


#### **SPACE Invader**

#### 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

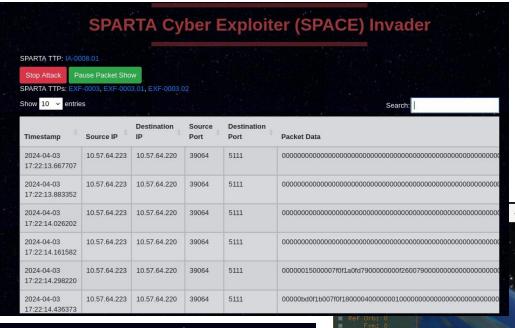


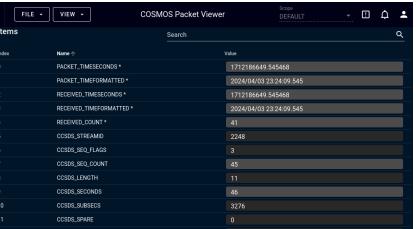


### **SPACE Invader (cont.)**

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
- Etc.



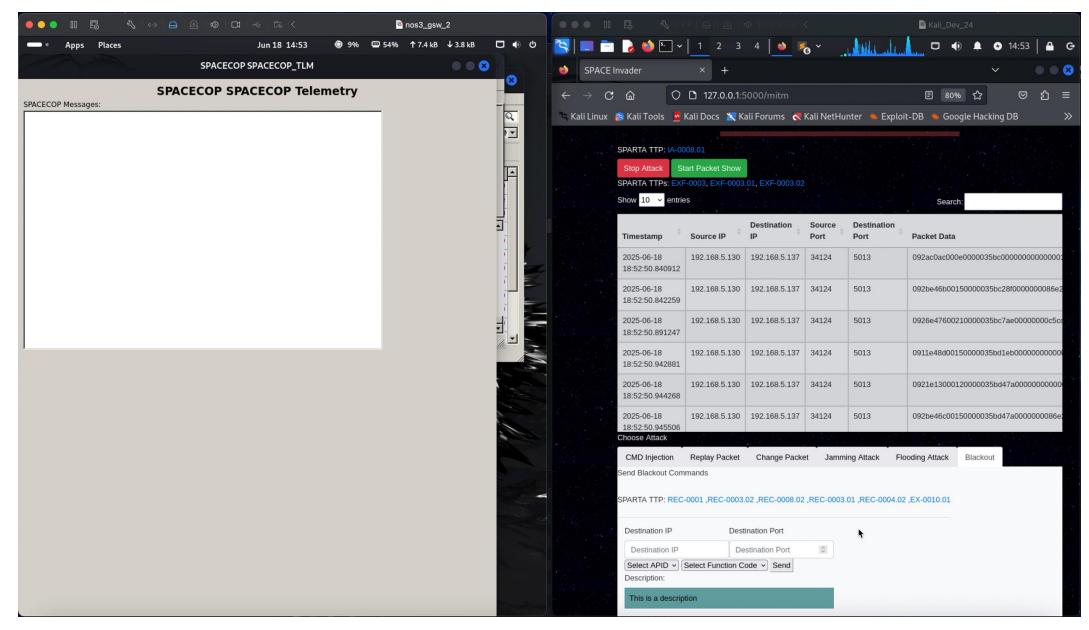




42 Unit Sphere Viewer

https://github.com/nasa/nos3

## **SpaceCOP Detecting Rogue App and Ransomware**





### **Detecting Onboard Malware, But it may be too late...**

#### Detection ≠ Mitigation

- As seen, SpaceCOP was able to detect the malware processes running, the files being modified and deleted, and system commands being executed
- However, the space operator may only be able to watch the alerts come down
  - Telemetry is only sent to the ground station when the spacecraft is within range
  - If these alerts were to come down as soon as spacecraft connects, the damage may already be done
- SpaceCOP and other IDS's are useful for seeing if an attack is taking place, not for preventing the attack from happening!
- IDS alone isn't enough in space -- detection without speed is irrelevant
  - Spacecraft cyber impacts can occur in seconds and waiting for ground review introduces critical delays that attackers exploit {ground loop is too slow}
- Mission failure doesn't wait for confirmation
- Persistent adversaries exploit delay
  - Sophisticated threats may stage attacks during ground contact gaps, safe-mode states, or reconfiguration windows where IDS alerts can't help fast enough.
- Detection ≠ Mitigation
  - An IDS may raise an alert, but if no autonomous action follows, mission-impacting behavior may complete before a human can intervene.

### **Automated Cyber Response Is No Longer Optional**

Spacecraft must respond in real time, integrating with FMS is key to mission continuity

- Automated response <u>is essential</u>
  - Spacecraft must be equipped to isolate faults, block malicious commands, or switch to safe configurations without waiting for ground input
- Integrating with Fault Management System (FMS) is critical
  - Cyber response must tie into existing fault management systems to avoid conflicts, reduce risk of false positives, and ensure mission continuity.
- Cyber must become a first-class spacecraft function
  - Like attitude control or thermal regulation, cyber defense must operate as a real-time onboard control system, not just a monitoring tool
- Call to action paper in November 2019 identified this

#### Intrusion Detection and Prevention Systems

The backbone of a cyber-resilient spacecraft should be a robust intrusion detection system (IDS). The IDS should consist of continuous monitoring of telemetry, command sequences, command receiver status, shared bus traffic, and flight software configuration and operating states. From a telemetry recommended course of action. If a severe rules violation occurs or a higher threshold is crossed, the spacecraft's intrusion prevention system (IPS) will take automated actions, which may include swapping to a redundant side, quarantining command sequences, reloading flight software, and/or halting suspect units. An example of the first

 SPARTA techniques and now IOBs support this position that attacks can occur and be detected but response is needed to assure mission continuity The IPS system should be integrated into the existing onboard spacecraft fault management system (FMS) because the FMS has its own fault detection and response system built in. Typically,

seen in operations. The reason that both the IPS and FMS systems should be integrated is that they are essentially performing the same functions but are looking for different anomaly signatures. In fact, there may be scenarios where each of them detects an anomalous condition and attempts to take an action. Having them integrated ensures they do not take conflicting actions.

The spacecraft IPS and the ground should retain the ability to return critical systems on the spacecraft to known cyber-safe mode. Cyber-safe mode is an operating mode of a spacecraft during which all

https://csps.aerospace.org/sites/default/files/2021-08/Bailey\_DefendingSpacecraft\_ 11052019.pdf



#### Conclusion

- Demonstrated that generic SPARTA IOBs work in real flight-like environments, but they need translation, integration, and automation to scale.
- ~200 IOBs across 10 behavioral categories now map to top 50 most critical SPARTA techniques (NRS-based).
- STIX patterning and automation (via DARS experiment) show that generic IOBs can become missionspecific rules.
- IDS is necessary but not sufficient
  - Onboard autonomous response is the next milestone
- What's next for the space industry
  - Integrate onboard machine learning to detect novel behaviors
  - Build Intrusion Prevention Systems (IPS) that respond autonomously
- Bottom Line: We're no longer theorizing space cyber we're building the real defenses.



#### https://sparta.aerospace.org





#### **Sample Media Links:**

- https://cyberscoop.com/space-satellite-cybersecurity-sparta/
- <a href="https://www.darkreading.com/ics-ot/space-race-defenses-satellite-cyberattacks">https://www.darkreading.com/ics-ot/space-race-defenses-satellite-cyberattacks</a>
- https://thecyberwire.com/podcasts/daily-podcast/1715/notes & https://thecyberwire.com/newsletters/signals-and-space/6/21

#### **Overview Briefings:**

- <u>Using SPARTA to Conduct Space Vehicle Cyber Assessments</u> (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: <a href="https://sparta.aerospace.org/resources/getting-started">https://sparta.aerospace.org/resources/getting-started</a> | <a href="https://sparta.aerospace.org/resources/getting-started/">https://sparta.aerospace.org/resources/getting-started</a>
- Understanding Space-Cyber TTPs with the SPARTA Matrix: <a href="https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix">https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix</a>
- Leveraging the SPARTA Matrix: <a href="https://aerospace.org/article/leveraging-sparta-matrix">https://aerospace.org/article/leveraging-sparta-matrix</a>
- Use Case w/ PCspooF:
  - <a href="https://aerospacecorp.medium.com/sparta-cyber-security-for-space-missions-4876f789e41c">https://aerospacecorp.medium.com/sparta-cyber-security-for-space-missions-4876f789e41c</a>
  - https://medium.com/the-aerospace-corporation/a-look-into-sparta-countermeasures-358e2fcd43ed
- FAQ: <a href="https://sparta.aerospace.org/resources/faq">https://sparta.aerospace.org/resources/faq</a>
- Matrix: <a href="https://sparta.aerospace.org">https://sparta.aerospace.org</a>
- Navigator: <a href="https://sparta.aerospace.org/navigator">https://sparta.aerospace.org/navigator</a> | Countermeasure Mapper: <a href="https://sparta.aerospace.org/countermeasures/mapper">https://sparta.aerospace.org/countermeasures/mapper</a>
- Notional Risk Scores on 5x5: <a href="https://sparta.aerospace.org/notional-risk-scores">https://sparta.aerospace.org/notional-risk-scores</a>
- Related Work: <a href="https://sparta.aerospace.org/related-work/did-space">https://sparta.aerospace.org/related-work/did-space</a> with ties into <a href="https://sparta.aerospace.org/related-work/did-space">TOR 2021-01333 REV A</a>
- <sup>23</sup> Indicators of Behavior: <a href="https://sparta.aerospace.org/related-work/iob">https://sparta.aerospace.org/related-work/iob</a>

#### Other Papers and Resources





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
- DEF CON 2024: From Theory to Reality: Demonstrating the Simplicity of SPARTA Attacks



- 2019: <u>Defending Spacecraft in the Cyber Domain</u>
- 2020: Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices
- 2021: Cybersecurity Protections for Spacecraft: A Threat Based Approach
- 2021: The Value of Space
- 2021: <u>Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles</u>
- 2022: Protecting Space Systems from Cyber Attack
- 2022: An International Technical Standard for Commercial Space System Cybersecurity A Call to Action
- 2024: Space Segment Cybersecurity Profile
- July 2022 Testimony: Space and Aeronautics Subcommittee Hearing Exploring Cyber Space:
   Cybersecurity for Civil and Commercial Space Systems
  - Video: <a href="https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964">https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964</a>
  - Written Testimony: <a href="https://republicans-science.house.gov/\_cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf">https://republicans-science.house.gov/\_cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf</a>



