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

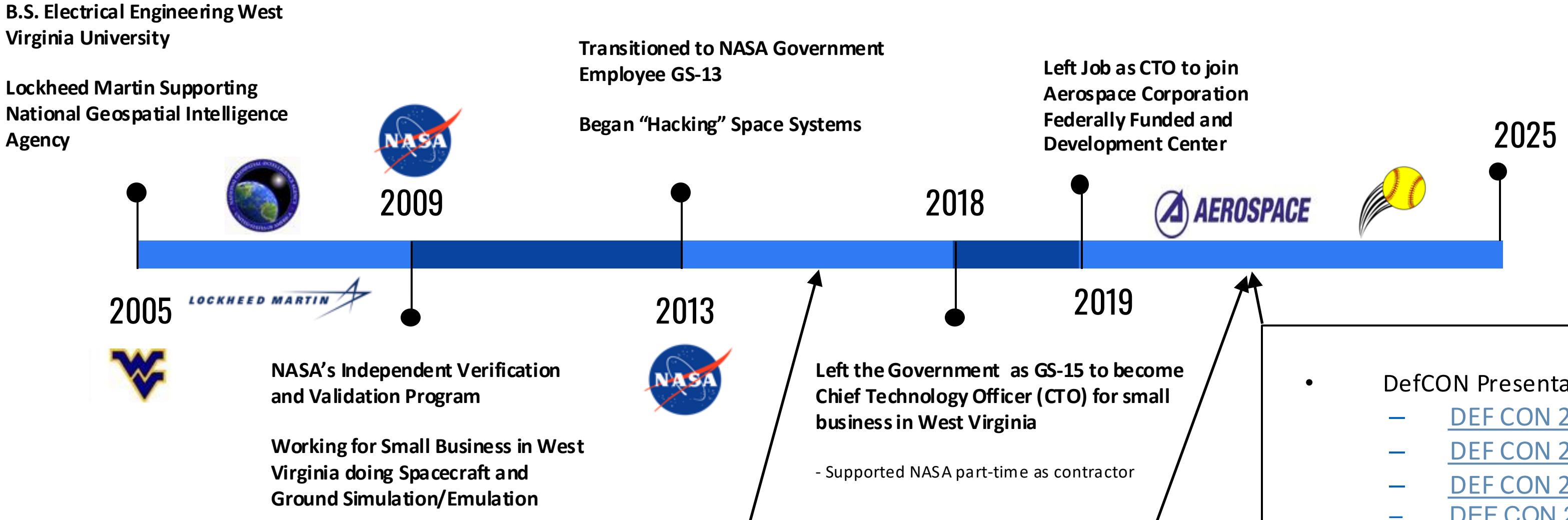
brandon.bailey@aero.org
randi.j.tinney@aero.org

Approved for Public Release – Derived from OTR 2022-01250, OTR-2024-00933 and OTR 2025-00882

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.



2005

B.S. Electrical Engineering West Virginia University

Lockheed Martin Supporting National Geospatial Intelligence Agency

2009

NASA's Independent Verification and Validation Program

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

2013

Transitioned to NASA Government Employee GS-13

Began "Hacking" Space Systems

2018

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

- Supported NASA part-time as contractor

2019

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

2025

Pen-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)
- 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

2019-2025

- 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: Defending Spacecraft in the Cyber Domain
  - 2020: Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices
  - 2021: Cybersecurity Protections for Spacecraft: A Threat Based Approach
  - 2022: Protecting Space Systems from Cyber Attack
  - 2024: Space Segment Cybersecurity Profile
- 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/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf
- SPARTA Launched
  - https://sparta.aerospace.org

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

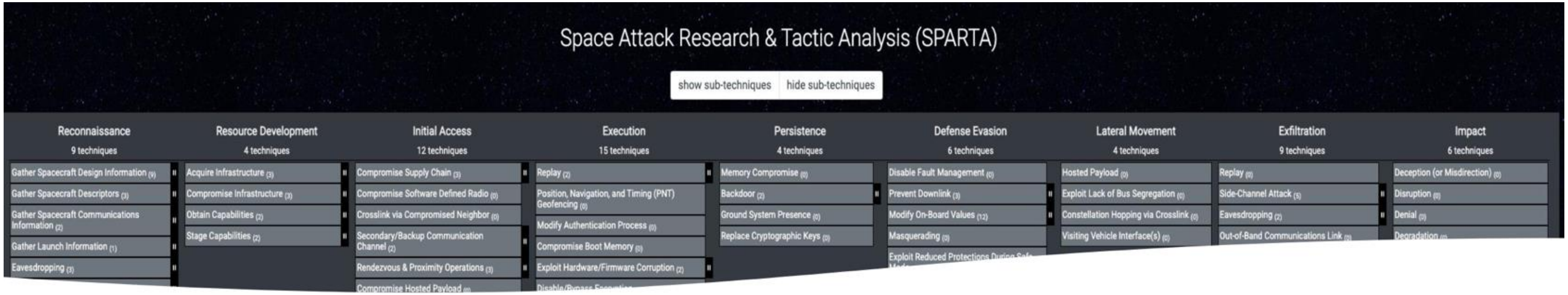
****** Also, Commercial Industry PenTest Consultant 2013-2024 (~75 tests)***

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

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**



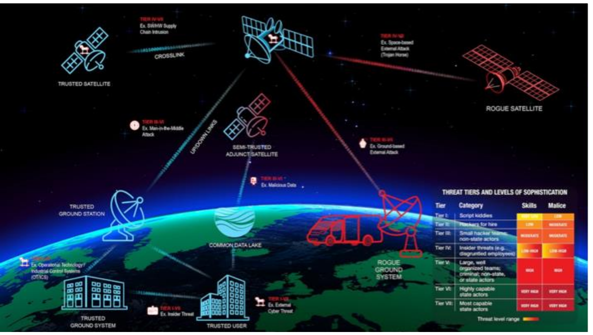
Space Attack Research & Tactic Analysis (SPARTA)

Reconnaissance 9 techniques	Resource Development 4 techniques	Initial Access 12 techniques	Execution 15 techniques	Persistence 4 techniques	Defense Evasion 6 techniques	Lateral Movement 4 techniques	Exfiltration 9 techniques	Impact 6 techniques
Gather Spacecraft Design Information (9)	Acquire Infrastructure (3)	Compromise Supply Chain (3)	Replay (2)	Memory Compromise (0)	Disable Fault Management (0)	Hosted Payload (0)	Replay (0)	Deception (or Misdirection) (0)
Gather Spacecraft Descriptors (3)	Compromise Infrastructure (3)	Compromise Software Defined Radio (0)	Position, Navigation, and Timing (PNT) Geofencing (0)	Backdoor (2)	Prevent Downlink (3)	Exploit Lack of Bus Segregation (0)	Side-Channel Attack (5)	Disruption (0)
Gather Spacecraft Communications Information (2)	Obtain Capabilities (2)	Crosslink via Compromised Neighbor (0)	Modify Authentication Process (0)	Ground System Presence (0)	Modify On-Board Values (12)	Constellation Hopping via Crosslink (0)	Eavesdropping (2)	Denial (0)
Gather Launch Information (1)	Stage Capabilities (2)	Secondary/Backup Communication Channel (2)	Compromise Boot Memory (0)	Replace Cryptographic Keys (0)	Masquerading (0)	Visiting Vehicle Interface(s) (0)	Out-of-Band Communications Link (0)	Degradation (0)
Eavesdropping (3)		Rendezvous & Proximity Operations (3)	Exploit Hardware/Firmware Corruption (2)		Exploit Reduced Protections During Safe-Mode			
		Compromise Hosted Payload (0)	Disable/Bypass Encryption					

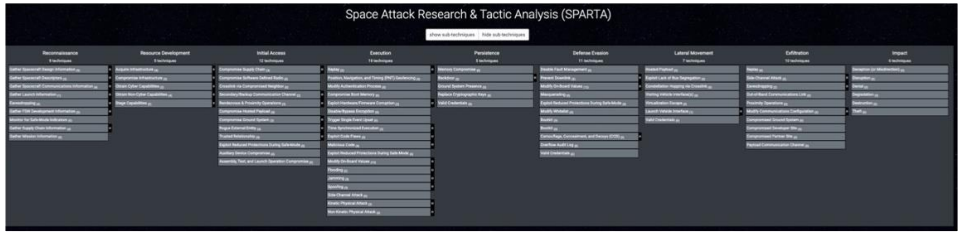
SPARTA provides threat-informed information to space professionals about how spacecraft may be compromised

Intel or Attacker Driven Countermeasure / Control / Requirement Derivation

Threat Intel → SPARTA Techniques → SPARTA Countermeasures → NIST SP 800-53 Controls

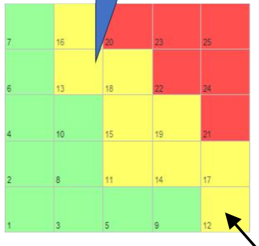

TRUSTED SATELLITE
CROSSLINK
Ex. SW/HW Supply Chain Intrusion
Ex. Space-based External Attack (Trojan Horse)
ROGUE SATELLITE
Ex. Man-in-the-Middle Attack
UP/DOWN LINKS
SEMI-TRUSTED ADJUNCT SATELLITE
Ex. Ground-based External Attack
Ex. Malicious Data
TRUSTED GROUND STATION
COMMON DATA LAKE
ROGUE GROUND SYSTEM
Ex. Operational Technology / Industrial Control Systems (OT/ICS)
TRUSTED GROUND SYSTEM
Ex. Insider Threat
TRUSTED USER
Ex. External Cyber Threat
THREAT TIERS AND LEVELS OF SOPHISTICATION
Tier
Category
Skills
Malice
Tier I: Script kiddies
Tier II: Hackers for hire
Tier III: Small hacker teams, non-state actors
Tier IV: Insider threats (e.g. disgruntled employees)
Tier V: Large, well organized teams; criminal; non-state, or state actors
Tier VI: Highly capable state actors
Tier VII: Most capable state actors
LOW
MODERATE
LOW-HIGH
HIGH
VERY HIGH
Threat level range

Decomposing Threats

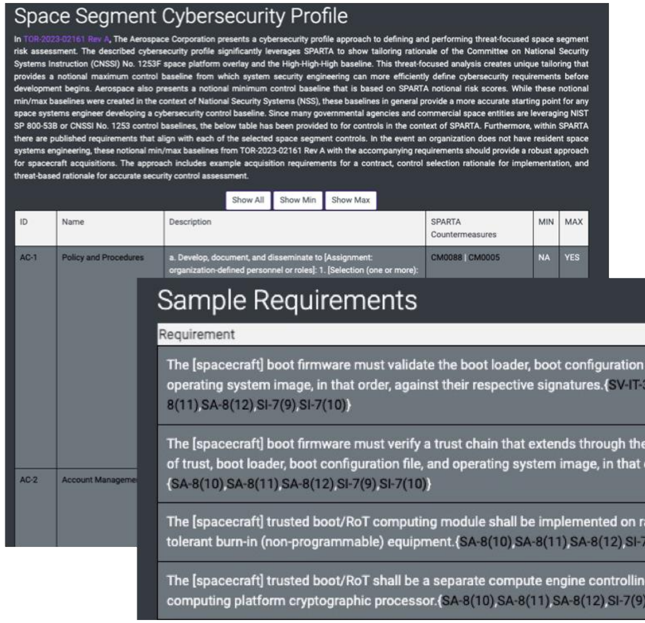


Mitigating Countermeasures

Controls &/or Requirements



7	16	20	23	25
6	13	18	22	24
4	10	15	19	21
2	8	11	14	17
1	3	5	9	12



Space Segment Cybersecurity Profile

In TOR-2023-02161 Rev A, The Aerospace Corporation presents a cybersecurity profile approach to defining and performing threat-focused space segment risk assessment. The described cybersecurity profile significantly leverages SPARTA to show tailoring rationale of the Committee on National Security Systems Instruction (CNSSI) No. 1253F space platform overlay and the High-High-High baseline. This threat-focused analysis creates unique tailoring that provides a notional maximum control baseline from which system security engineering can more efficiently define cybersecurity requirements before development begins. Aerospace also presents a notional minimum control baseline that is based on SPARTA notional risk scores. While these notional min/max baselines were created in the context of National Security Systems (NSS), these baselines in general provide a more accurate starting point for any space systems engineer developing a cybersecurity control baseline. Since many governmental agencies and commercial space entities are leveraging NIST SP 800-53B or CNSSI No. 1253 control baselines, the below table has been provided to for controls in the context of SPARTA. Furthermore, within SPARTA there are published requirements that align with each of the selected space segment controls. In the event an organization does not have resident space systems engineering, these notional min/max baselines from TOR-2023-02161 Rev A with the accompanying requirements should provide a robust approach for spacecraft acquisitions. The approach includes example acquisition requirements for a contract, control selection rationale for implementation, and threat-based rationale for accurate security control assessment.

Show All | Show Min | Show Max

ID	Name	Description	SPARTA Countermeasures	MIN	MAX
AC-1	Policy and Procedures	a. Develop, document, and disseminate to [Assignment: organization-defined personnel or roles]: 1. [Selection (one or more):	CM0088 | CM0005	NA	YES
AC-2	Account Manageme				

Sample Requirements

Requirement
The [spacecraft] boot firmware must validate the boot loader, boot configuration operating system image, in that order, against their respective signatures.{SV-IT-3 8(11),SA-8(12),SI-7(9),SI-7(10)}
The [spacecraft] boot firmware must verify a trust chain that extends through the of trust, boot loader, boot configuration file, and operating system image, in that {SA-8(10),SA-8(11),SA-8(12),SI-7(9),SI-7(10)}
The [spacecraft] trusted boot/RoT computing module shall be implemented on r tolerant burn-in (non-programmable) equipment.{SA-8(10),SA-8(11),SA-8(12),SI-7
The [spacecraft] trusted boot/RoT shall be a separate compute engine controllin computing platform cryptographic processor.{SA-8(10),SA-8(11),SA-8(12),SI-7(9)

Impact | Likelihood

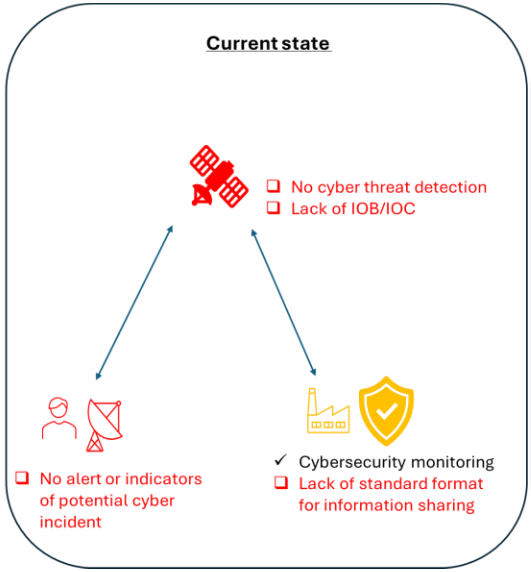
Impact | Vulnerabilities | Threats → Risk

informs

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

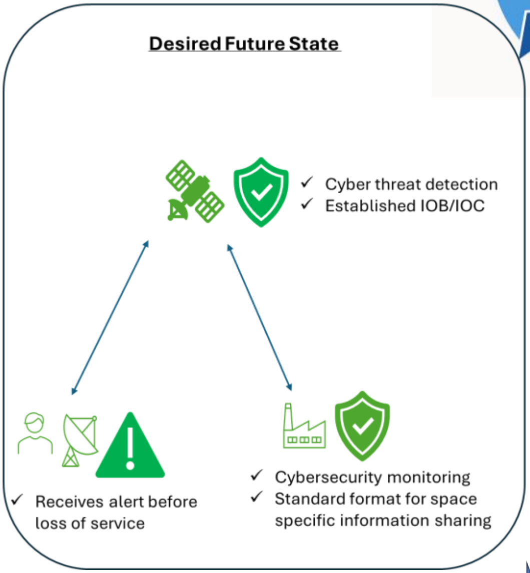
Similar Process Applies for IOBs/Detection Engineering

Translating Techniques to Detections



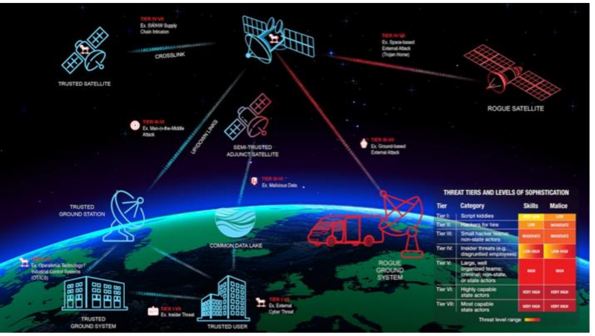
Current state

- ❑ No cyber threat detection
- ❑ Lack of IOB/IOC
- ❑ No alert or indicators of potential cyber incident
- ✓ Cybersecurity monitoring
- ❑ Lack of standard format for information sharing



Desired Future State

- ✓ Cyber threat detection
- ✓ Established IOB/IOC
- ✓ Receives alert before loss of service
- ✓ Cybersecurity monitoring
- ✓ Standard format for space specific information sharing

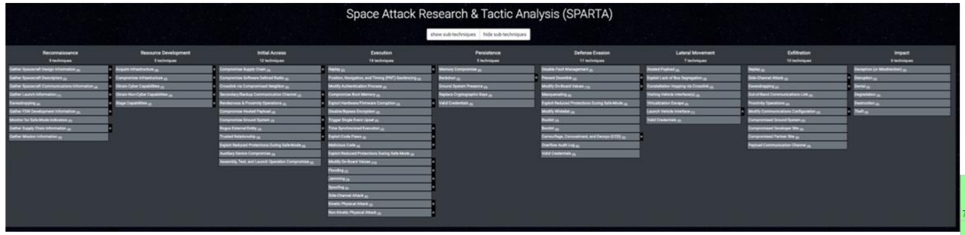

TIER IV-VII
Ex. SW/HW Supply Chain Intrusion
CROSSLINK
TRUSTED SATELLITE
TIER IV-VII
Ex. Space-based External Attack (Trojan Horse)
ROGUE SATELLITE
TIER III-VI
Ex. Man-in-the-Middle Attack
UP/DOWN LINKS
SEMI-TRUSTED ADJUNCT SATELLITE
TIER III-VII
Ex. Ground-based External Attack
TIER III-VI
Ex. Malicious Data
TRUSTED GROUND STATION
COMMON DATA LAKE
ROGUE GROUND SYSTEM
Ex. Operational Technology/ Industrial Control Systems (OT/ICS)
TRUSTED GROUND SYSTEM
TIER I-VII
Ex. Insider Threat
TRUSTED USER
TIER I-VII
Ex. External Cyber Threat

THREAT TIERS AND LEVELS OF SOPHISTICATION

Tier	Category	Skills	Malice
Tier I:	Script kiddies	VERY LOW	LOW
Tier II:	Hackers for hire	LOW	MODERATE
Tier III:	Small hacker teams; non-state actors	MODERATE	MODERATE
Tier IV:	Insider threats (e.g. disgruntled employees)	LOW-HIGH	LOW-HIGH
Tier V:	Large, well organized teams; criminal; non-state, or state actors	HIGH	HIGH
Tier VI:	Highly capable state actors	VERY HIGH	VERY HIGH
Tier VII:	Most capable state actors	VERY HIGH	VERY HIGH

Threat level range

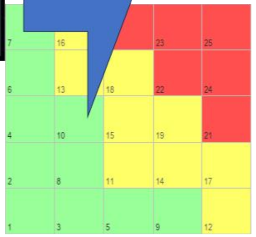
Decomposing Threats



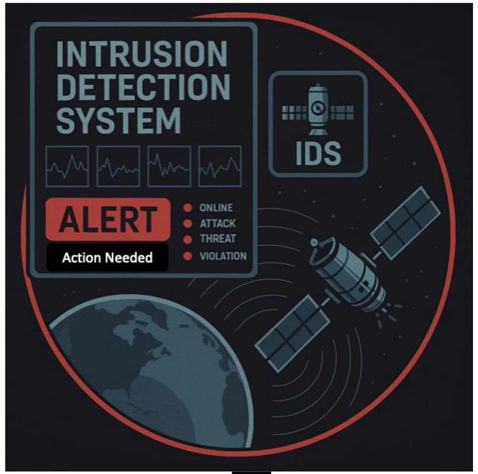
Space Attack Research & Tactic Analysis (SPARTA)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Defense Evasion	Lateral Movement	Exfiltration	Impact
9 techniques	5 techniques	12 techniques	18 techniques	5 techniques	11 techniques	7 techniques	10 techniques	6 techniques
Gather Spacecraft Design Information	Acquire Infrastructure	Compromise Supply Chain	Replay	Memory Compromise	Disable Fault Management	Hosted Payload	Replay	Deception (or Misdirection)
Gather Spacecraft Descriptors	Compromise Infrastructure	Compromise Software Defined Radio	Position, Navigation, and Timing (PNT) Geofencing	Backdoor	Prevent Downlink	Exploit Lack of Bus Segregation	Side-Channel Attack	Disruption
Gather Spacecraft Communications Information	Obtain Cyber Capabilities	Crosslink via Compromised Neighbor	Modify Authentication Process	Ground System Presence	Modify On-Board Values	Constellation Hopping via Crosslink	Eavesdropping	Denial
Gather Launch Information	Obtain Non-Cyber Capabilities	Secondary/Backup Communication Channel	Compromise Boot Memory	Replace Cryptographic Keys	Masquerading	Visiting Vehicle Interface(s)	Out-of-Band Communications Link	Degradation
Eavesdropping	Stage Capabilities	Rendezvous & Proximity Operations	Exploit Hardware/Firmware Corruption	Valid Credentials	Exploit Reduced Protections During Safe-Mode	Virtualization Escape	Proximity Operations	Destruction
Gather FSW Development Information		Compromise Hosted Payload	Disable/Bypass Encryption		Modify Whitelist	Launch Vehicle Interface	Modify Communications Configuration	Theft
Monitor for Safe-Mode Indicators		Compromise Ground System	Trigger Single Event Upset		Rootkit	Valid Credentials	Compromised Ground System	
Gather Supply Chain Information		Rogue External Entity	Time Synchronized Execution		Bootkit		Compromised Developer Site	
Gather Mission Information		Trusted Relationship	Exploit Code Flaws		Camouflage, Concealment, and Decoys (CCD)		Compromised Partner Site	
		Exploit Reduced Protections During Safe-Mode	Malicious Code		Overflow Audit Log		Payload Communication Channel	
		Auxiliary Device Compromise	Exploit Reduced Protections During Safe-Mode		Valid Credentials			
		Assembly, Test, and Launch Operation Compromise	Modify On-Board Values					
			Flooding					
			Jamming					
			Spoofing					
			Side-Channel Attack					
			Kinetic Physical Attack					
			Non-Kinetic Physical Attack					

IOBs



7	16		23	25
6	13	18	22	24
4	10	15	19	21
2	8	11	14	17
1	3	5	9	12



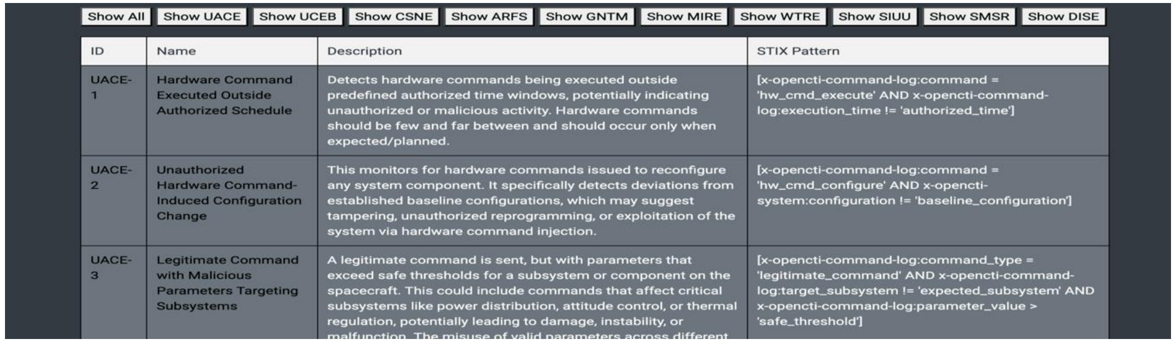
Inform Ground

SPARTA Indicators of Behavior (IOBs) – Launched April 2025

A crucial element in modern spacecraft defense

- Funded by the Department of Homeland Security (DHS) Science and Technology (S&T) Directorate 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: https://medium.com/the-aerospace-corporation/indicators-of-behavior-iobs-in-sparta-v3-0-c42ab0683100
- 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



ID	Name	Description	STIX Pattern
UACE-1	Hardware Command Executed Outside Authorized Schedule	Detects hardware commands being executed outside predefined authorized time windows, potentially indicating unauthorized or malicious activity. Hardware commands should be few and far between and should occur only when expected/planned.	[x-opencti-command-log:command = 'hw_cmd_execute' AND x-opencti-command-log:execution_time != 'authorized_time']
UACE-2	Unauthorized Hardware Command-Induced Configuration Change	This monitors for hardware commands issued to reconfigure any system component. It specifically detects deviations from established baseline configurations, which may suggest tampering, unauthorized reprogramming, or exploitation of the system via hardware command injection.	[x-opencti-command-log:command = 'hw_cmd_configure' AND x-opencti-system:configuration != 'baseline_configuration']
UACE-3	Legitimate Command with Malicious Parameters Targeting Subsystems	A legitimate command is sent, but with parameters that exceed safe thresholds for a subsystem or component on the spacecraft. This could include commands that affect critical subsystems like power distribution, attitude control, or thermal regulation, potentially leading to damage, instability, or malfunction. The misuse of valid parameters across different	[x-opencti-command-log:command_type = 'legitimate_command' AND x-opencti-command-log:target_subsystem != 'expected_subsystem' AND x-opencti-command-log:parameter_value > 'safe_threshold']

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

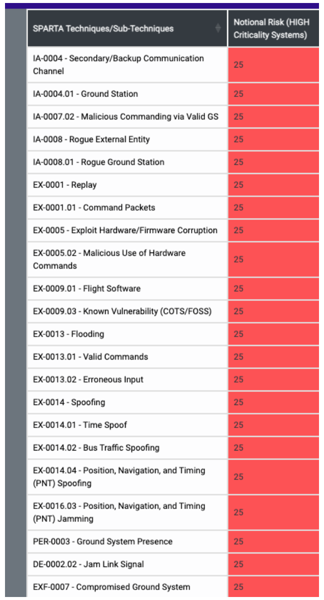
In this first iteration, ~200 IOBs were created

Generating SPARTA's Initial IOBs

Red informing Blue

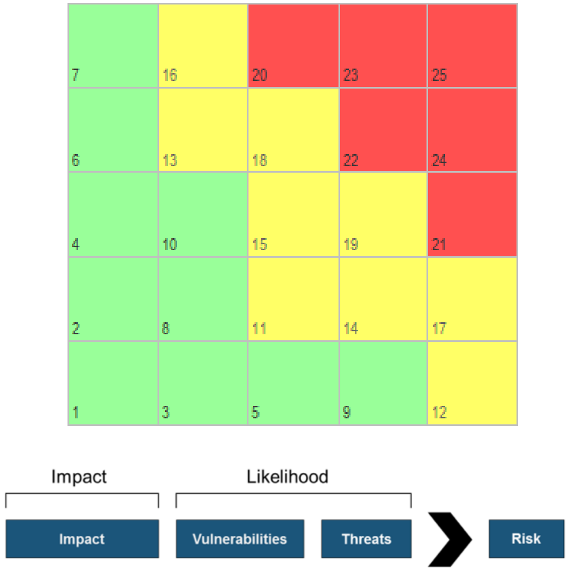
- Turning theory into detection: we didn't just theorize, we attacked
  - We applied real SPARTA techniques against flight-like systems to observe what adversary behavior ***actually looks like*** on a spacecraft.
- From red team to real defenses, offensive testing revealed how attacks manifest in data which informs the design of IOBs tailored to actual spacecraft subsystems
- SPARTA gave us the threats/techniques
  - Risk-ranked techniques (NRS - https://sparta.aerospace.org/notional-risk-scores) 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.

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

⋮



7	16	20	23	25
6	13	18	22	24
4	10	15	19	21
2	8	11	14	17
1	3	5	9	12

SPARTA’s IOB Behavioral Categories

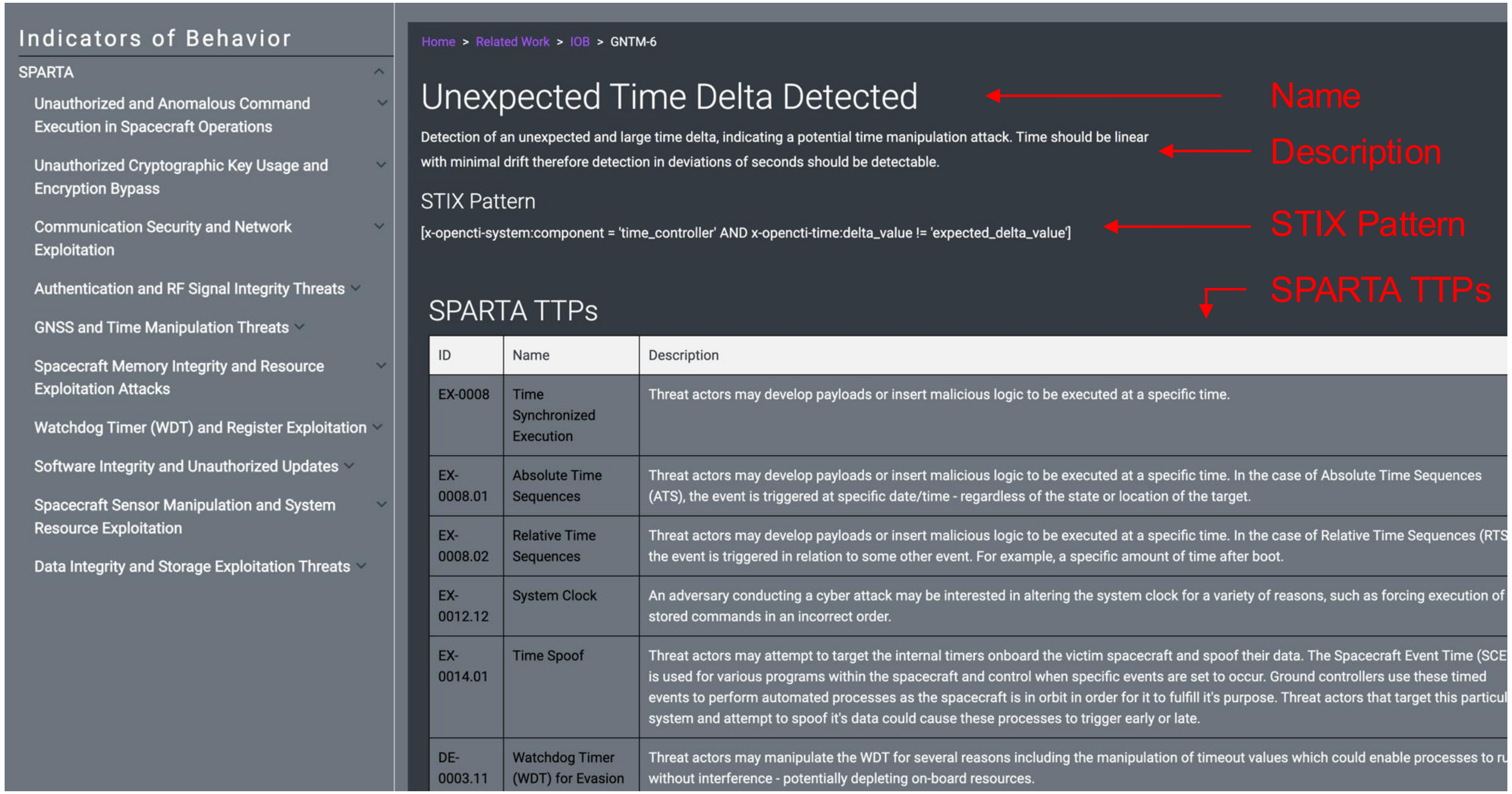
~200 IOBs Fall into 10 Categories

- 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



Indicators of Behavior
SPARTA
Unauthorized and Anomalous Command Execution in Spacecraft Operations
Unauthorized Cryptographic Key Usage and Encryption Bypass
Communication Security and Network Exploitation
Authentication and RF Signal Integrity Threats
GNSS and Time Manipulation Threats
Spacecraft Memory Integrity and Resource Exploitation Attacks
Watchdog Timer (WDT) and Register Exploitation
Software Integrity and Unauthorized Updates
Spacecraft Sensor Manipulation and System Resource Exploitation
Data Integrity and Storage Exploitation Threats
Home > Related Work > IOB > GNTM-6

Unexpected Time Delta Detected

Detection of an unexpected and large time delta, indicating a potential time manipulation attack. Time should be linear with minimal drift therefore detection in deviations of seconds should be detectable.

STIX Pattern

[x-opencti-system:component = 'time_controller' AND x-opencti-time:delta_value != 'expected_delta_value']

SPARTA TTPs

ID	Name	Description
EX-0008	Time Synchronized Execution	Threat actors may develop payloads or insert malicious logic to be executed at a specific time.
EX-0008.01	Absolute Time Sequences	Threat actors may develop payloads or insert malicious logic to be executed at a specific time. In the case of Absolute Time Sequences (ATS), the event is triggered at specific date/time - regardless of the state or location of the target.
EX-0008.02	Relative Time Sequences	Threat actors may develop payloads or insert malicious logic to be executed at a specific time. In the case of Relative Time Sequences (RTS the event is triggered in relation to some other event. For example, a specific amount of time after boot.
EX-0012.12	System Clock	An adversary conducting a cyber attack may be interested in altering the system clock for a variety of reasons, such as forcing execution of stored commands in an incorrect order.
EX-0014.01	Time Spoof	Threat actors may attempt to target the internal timers onboard the victim spacecraft and spoof their data. The Spacecraft Event Time (SCE is used for various programs within the spacecraft and control when specific events are set to occur. Ground controllers use these timed events to perform automated processes as the spacecraft is in orbit in order for it to fulfill it's purpose. Threat actors that target this particul system and attempt to spoof it's data could cause these processes to trigger early or late.
DE-0003.11	Watchdog Timer (WDT) for Evasion	Threat actors may manipulate the WDT for several reasons including the manipulation of timeout values which could enable processes to ru without interference - potentially depleting on-board resources.

Name

Description

STIX Pattern

SPARTA TTPs

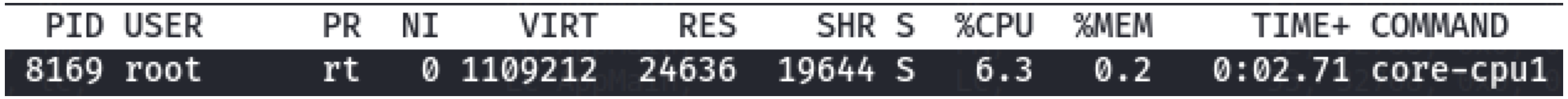
Can developer who did not create the IOBs interpret and develop detection on a spacecraft?

IDS Experiment Setup

Initial Proof of Concept – Testing the Theory

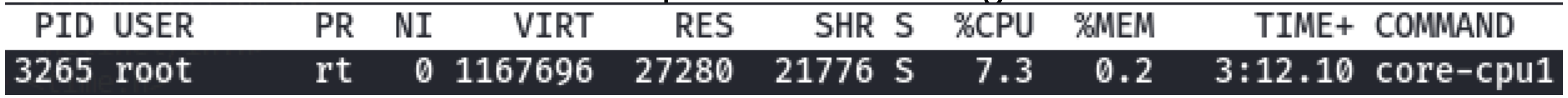
- Utilizing NASA’s NOS3 open-source and free digital twin
  - cFS utilized for spacecraft software (Coded in C)
  - COSMOS utilized for ground station (Coded in Ruby)
- IDS (SpaceCOP) migrated to a cFS application that runs on-board the spacecraft within the FSW
  - Features ~30 different SPARTA IOB 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 USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
3265 root      rt   0 1167696  27280  21776 S   7.3   0.2   3:12.10 core-cpu1
```

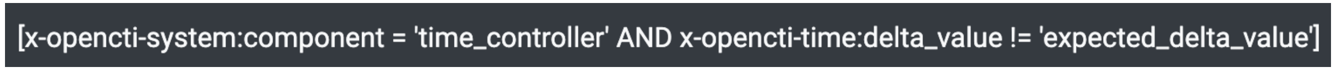
NASA’s NOS3: https://github.com/nasa/nos3

Aerospace’s SpaceCOP: https://aerospace.org/article/cybersecurity-orbit-how-aerospace-evolving-defenses-against-emerging-space-threats

IDS Experiment Setup (cont.)

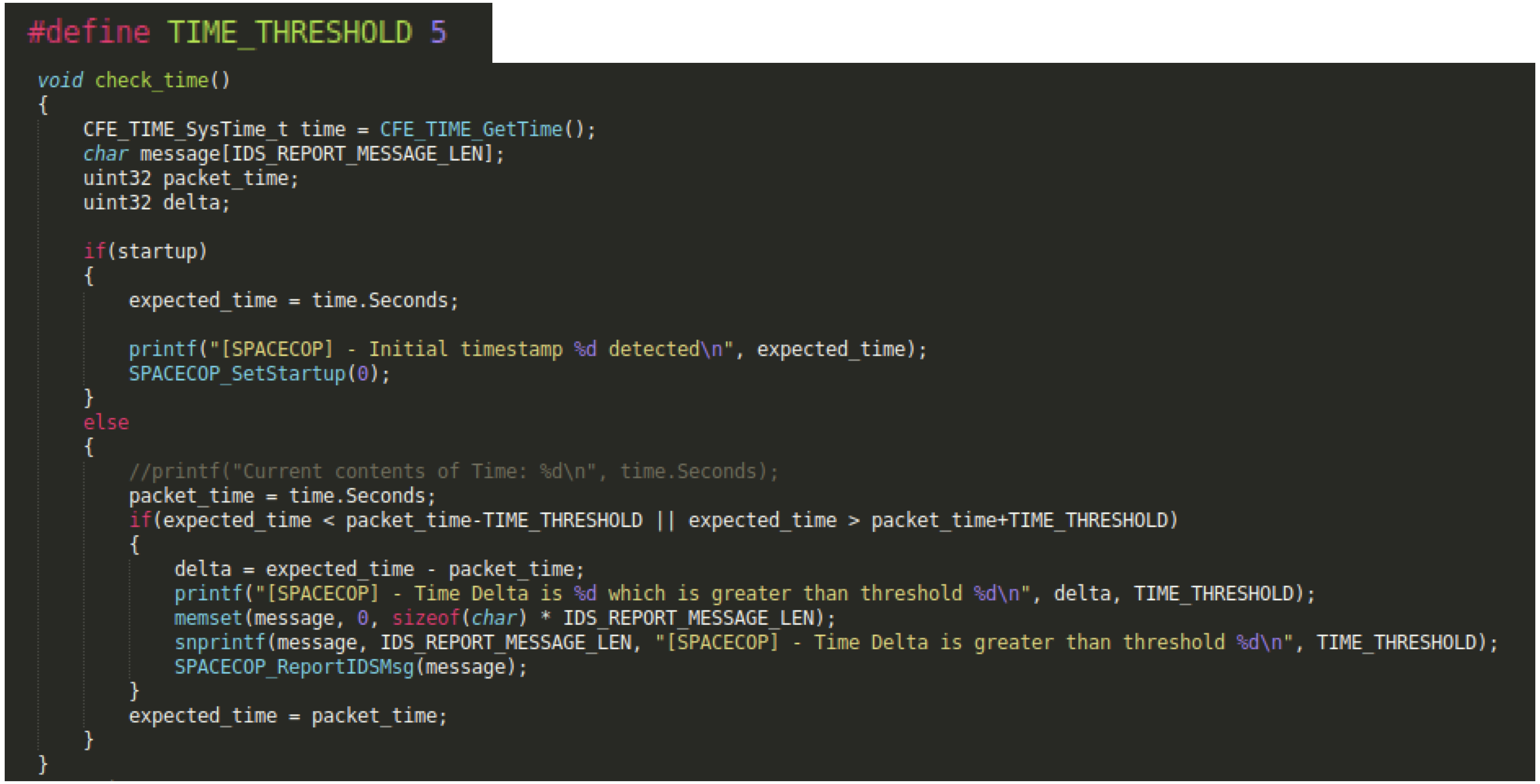
Unexpected Time Delta Detected IOB Example

- Unexpected Time Delta IDS detection code within SpaceCOP
- Define TIME_THRESHOLD
  - Initializes at 5 seconds but can be changed via command sent from ground station later



```
[x-opencti-system:component = 'time_controller' AND x-opencti-time:delta_value != 'expected_delta_value']
```

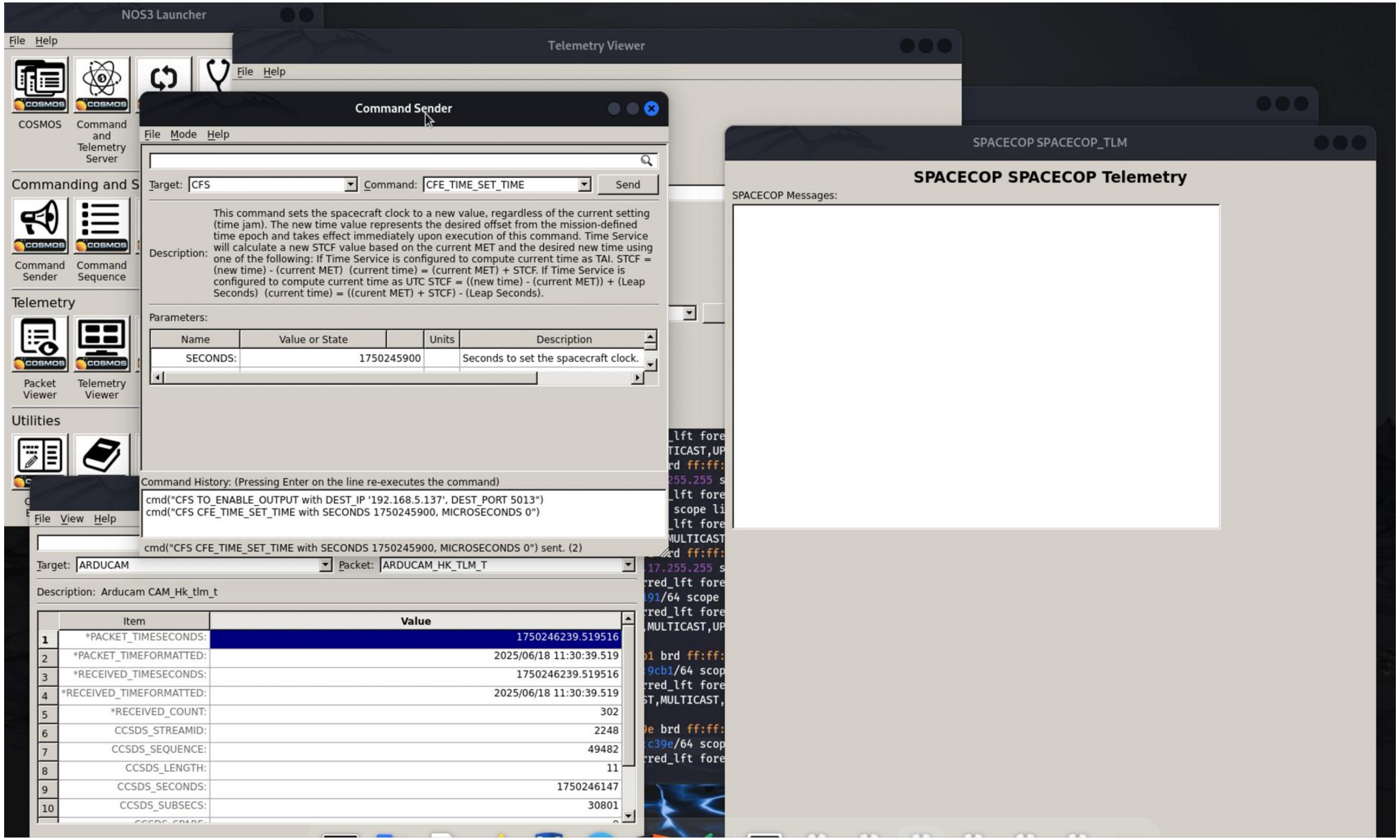
- Gets time via cFS API call (CFE_TIME_GetTime)
- If system is first starting up, store the seconds in “expected_time” value
- Else, see if the current seconds +/- defined TIME_THRESHOLD is larger than the “expected_time”
- If so, report the time delta is unexpected
- Store the current seconds for next iteration



```c
#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);
    }
    else
    {
        //printf("Current contents of Time: %d\n", time.Seconds);
        packet_time = time.Seconds;
        if(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



Target: CFS Command: CFE_TIME_SET_TIME

Description: This command sets the spacecraft clock to a new value, regardless of the current setting (time jam). The new time value represents the desired offset from the mission-defined time epoch and takes effect immediately upon execution of this command. Time Service will calculate a new STCF value based on the current MET and the desired new time using one of the following: If Time Service is configured to compute current time as TAI. STCF = (new time) - (current MET) (current time) = (current MET) + STCF. If Time Service is configured to compute current time as UTC STCF = ((new time) - (current MET)) + (Leap Seconds) (current time) = ((curent MET) + STCF) - (Leap Seconds).

Parameters:

Name	Value or State		Units	Description
SECONDS:	1750245900			Seconds to set the spacecraft clock.

Command History: (Pressing Enter on the line re-executes the command)

```
cmd("CFS TO_ENABLE_OUTPUT with DEST_IP '192.168.5.137', DEST_PORT 5013")
cmd("CFS CFE_TIME_SET_TIME with SECONDS 1750245900, MICROSECONDS 0")
```

```
cmd("CFS CFE_TIME_SET_TIME with SECONDS 1750245900, MICROSECONDS 0") sent. (2)
```

SPACECOP SPACECOP Telemetry

SPACECOP Messages:

Target: ARDUCAM Packet: ARDUCAM_HK_TLM_T

Description: Arducam CAM_Hk_tlm_t

	Item	Value
1	*PACKET_TIMESECONDS:	1750246239.519516
2	*PACKET_TIMEFORMATTED:	2025/06/18 11:30:39.519
3	*RECEIVED_TIMESECONDS:	1750246239.519516
4	*RECEIVED_TIMEFORMATTED:	2025/06/18 11:30:39.519
5	*RECEIVED_COUNT:	302
6	CCSDS_STREAMID:	2248
7	CCSDS_SEQUENCE:	49482
8	CCSDS_LENGTH:	11
9	CCSDS_SECONDS:	1750246147
10	CCSDS_SUBSECS:	30801

[SPARTA TTP (e.g., EX-0014.01)]
↓ (used in red team exploitation)
[Real Attack Observed]
↓ (telemetry & command anomalies collected)
[Behavior Modeled as IOB]
↓ (engineered detection logic)
[STIX Pattern Created]
↓ (IDS Rule Implemented)
[Detection Validated in FlatSat]

Experiment Worked Once…

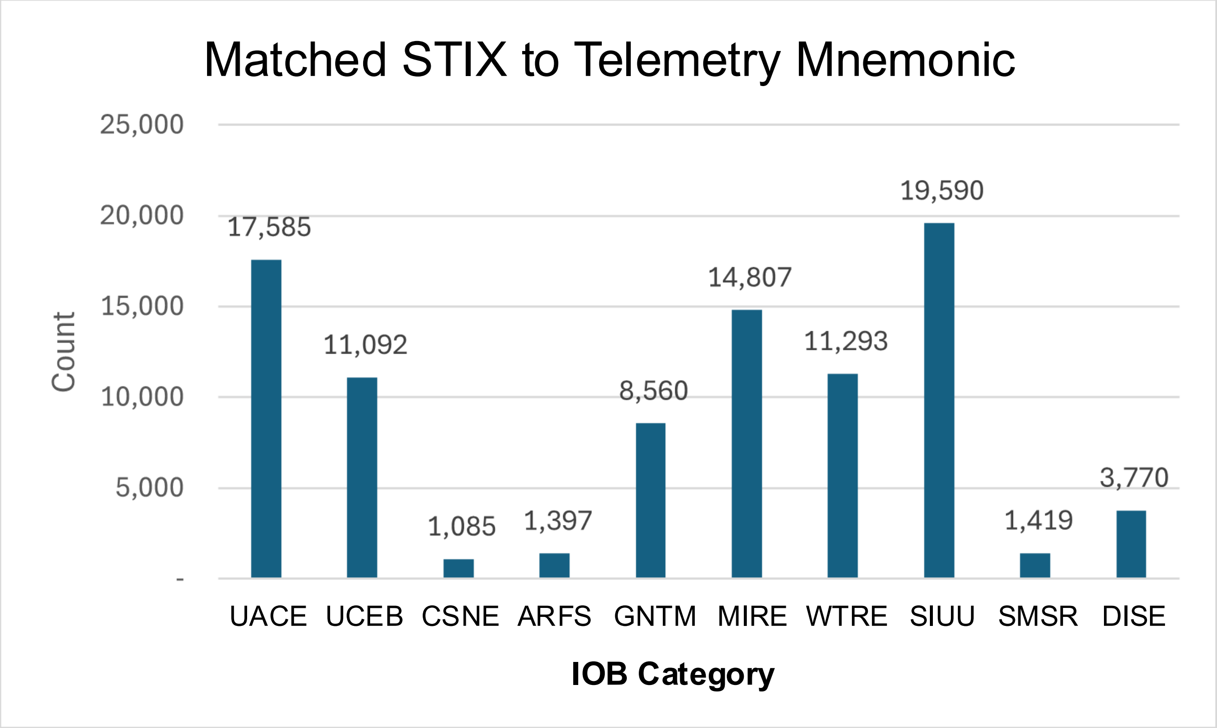
Do the IOBs Scale?

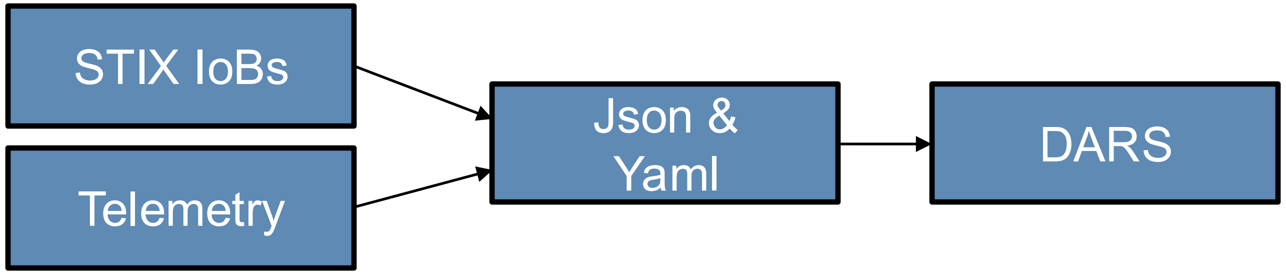
- After applying on a small subset of IOBs successfully, we asked:
  Does this scale? Can *all* SPARTA IOBs translate into real, mission-specific data?
- The challenge
  - SPARTA IOBs are designed to be generic, but can they be mapped to actual telemetry, command logs, and onboard activity?
- We know translation is needed
  - Mapping STIX-based IOBs to spacecraft-specific data (e.g., telemetry mnemonics, onboard processes, message formats) 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 IoBs**
  - 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

https://aerospace.org/fact-sheet/detection-and-reporting-system-dars-fact-sheet

Beyond Theory: Testing IOBs Against Advanced Threats

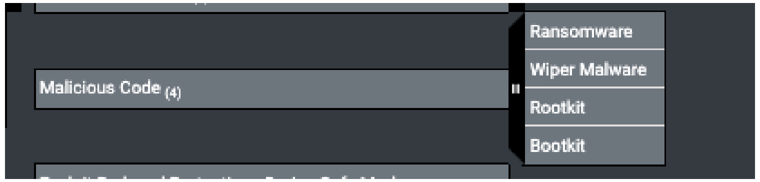
Detecting Actual Malware and Advanced Persistent Threats Onboard

- 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

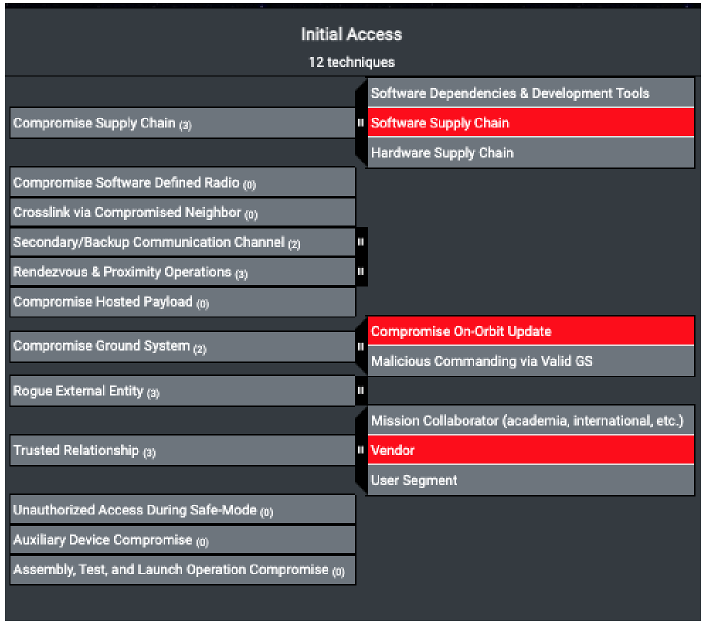


Malicious Code (4)

- Ransomware
- Wiper Malware
- Rootkit
- Bootkit

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

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



Initial Access

12 techniques

Compromise Supply Chain (3)
- Software Dependencies & Development Tools
- Software Supply Chain
- Hardware Supply Chain

Compromise Software Defined Radio (0)

Crosslink via Compromised Neighbor (0)

Secondary/Backup Communication Channel (2)

Rendezvous & Proximity Operations (3)

Compromise Hosted Payload (0)

Compromise Ground System (2)
- Compromise On-Orbit Update
- Malicious Commanding via Valid GS

Rogue External Entity (3)

Trusted Relationship (3)
- Mission Collaborator (academia, international, etc.)
- Vendor
- User Segment

Unauthorized Access During Safe-Mode (0)

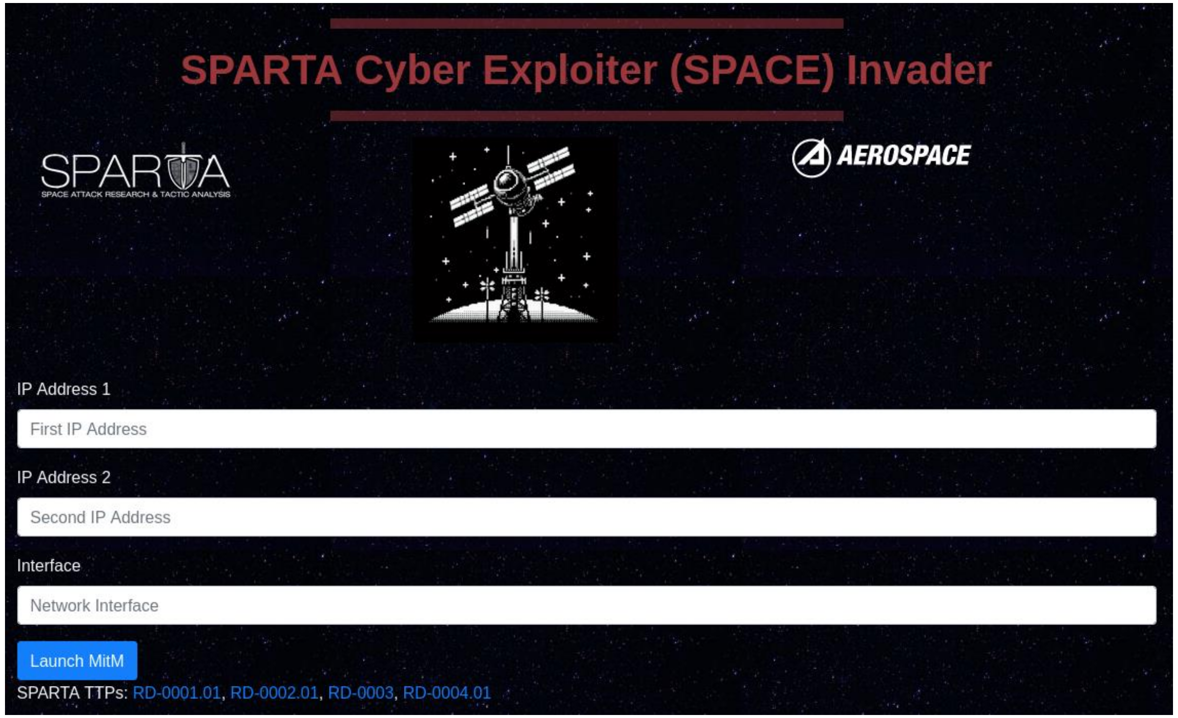
Auxiliary Device Compromise (0)

Assembly, Test, and Launch Operation Compromise (0)

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



SPARTA Cyber Exploiter (SPACE) Invader

IP Address 1

First IP Address

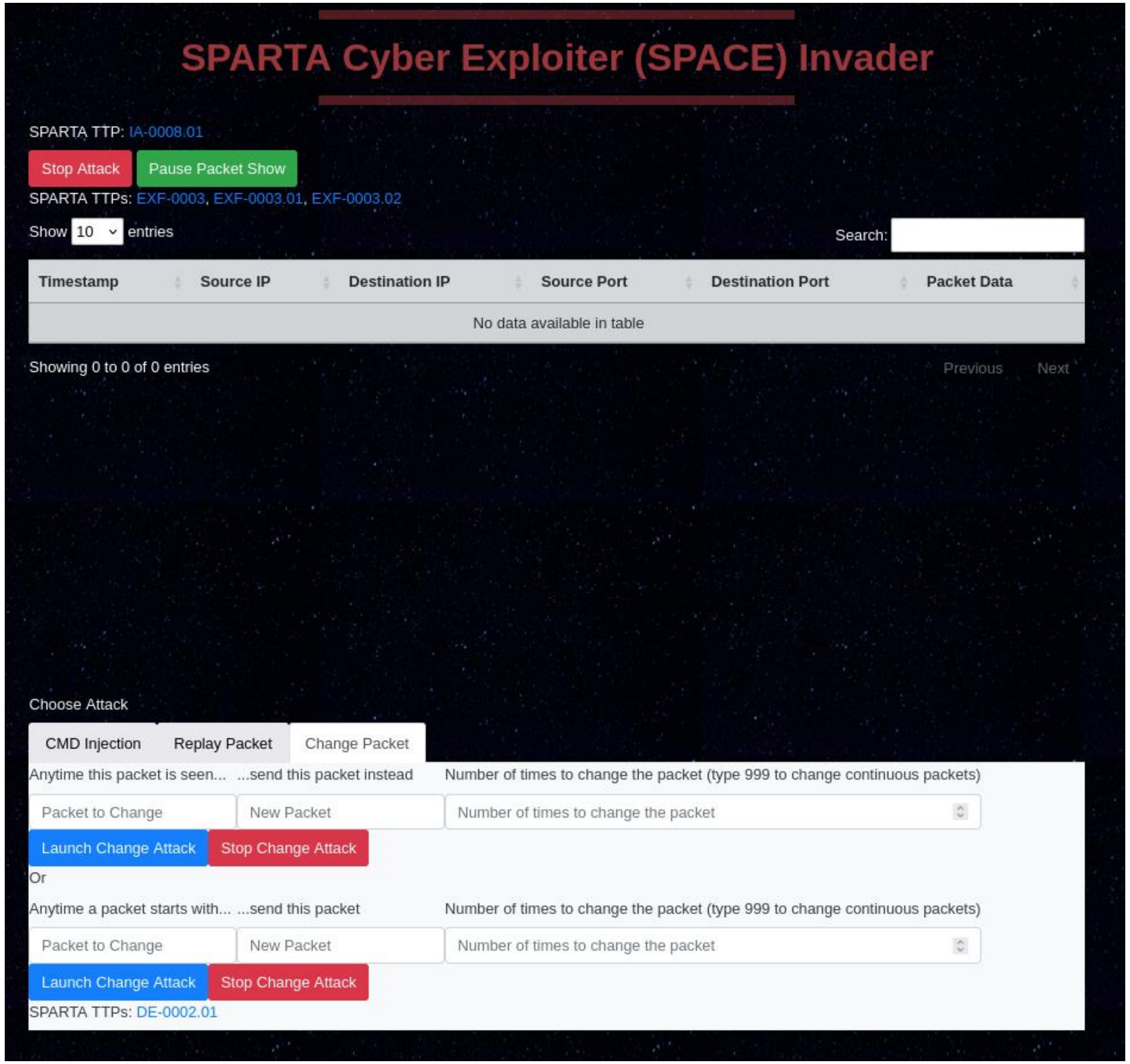
IP Address 2

Second IP Address

Interface

Network Interface

SPARTA TTPs: RD-0001.01, RD-0002.01, RD-0003, RD-0004.01



SPARTA Cyber Exploiter (SPACE) Invader

SPARTA TTP: IA-0008.01

SPARTA TTPs: EXF-0003, EXF-0003.01, EXF-0003.02

Show 10 entries

Search:

Timestamp	Source IP	Destination IP	Source Port	Destination Port	Packet Data
No data available in table					

Showing 0 to 0 of 0 entries

Choose Attack

Anytime this packet is seen... ...send this packet instead Number of times to change the packet (type 999 to change continuous packets)

Packet to Change | New Packet | Number of times to change the packet

Or

Anytime a packet starts with... ...send this packet Number of times to change the packet (type 999 to change continuous packets)

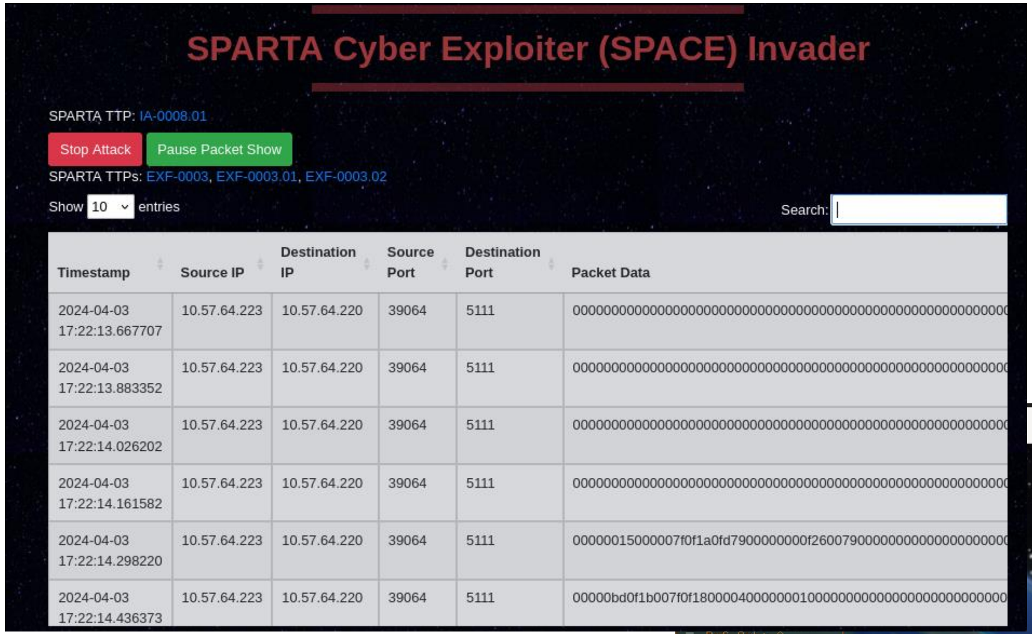
Packet to Change | New Packet | Number of times to change the packet

SPARTA TTPs: DE-0002.01

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.

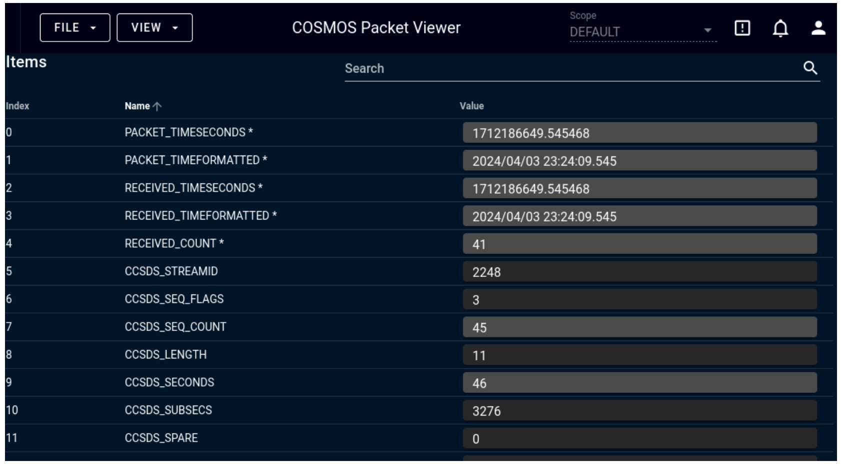


SPARTA Cyber Exploiter (SPACE) Invader

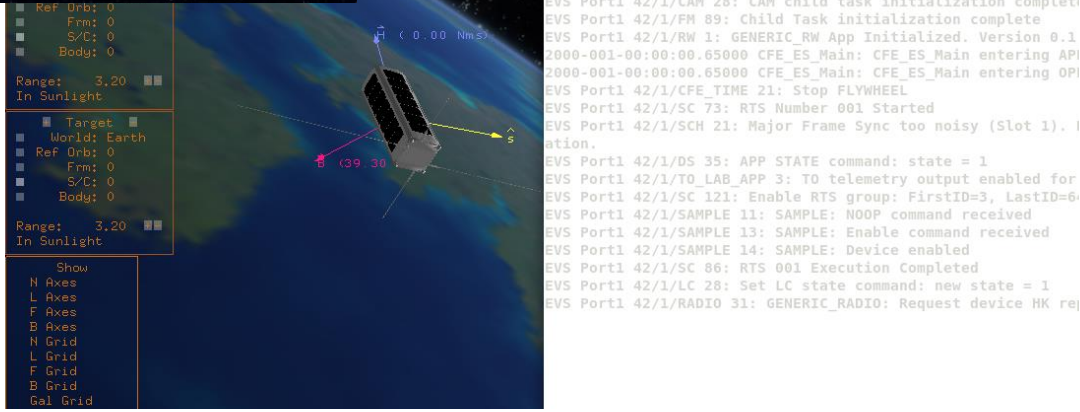
SPARTA TTP: IA-0008.01

SPARTA TTPs: EXF-0003, EXF-0003.01, EXF-0003.02

Timestamp	Source IP	Destination IP	Source Port	Destination Port	Packet Data
2024-04-03 17:22:13.667707	10.57.64.223	10.57.64.220	39064	5111	000000000000000000000000000000000000000000000000000000000000
2024-04-03 17:22:13.883352	10.57.64.223	10.57.64.220	39064	5111	000000000000000000000000000000000000000000000000000000000000
2024-04-03 17:22:14.026202	10.57.64.223	10.57.64.220	39064	5111	000000000000000000000000000000000000000000000000000000000000
2024-04-03 17:22:14.161582	10.57.64.223	10.57.64.220	39064	5111	000000000000000000000000000000000000000000000000000000000000
2024-04-03 17:22:14.298220	10.57.64.223	10.57.64.220	39064	5111	00000015000007f0f1a0fd7900000000f260079000000000000000000000
2024-04-03 17:22:14.436373	10.57.64.223	10.57.64.220	39064	5111	00000bd0f1b007f0f18000040000000100000000000000000000000000



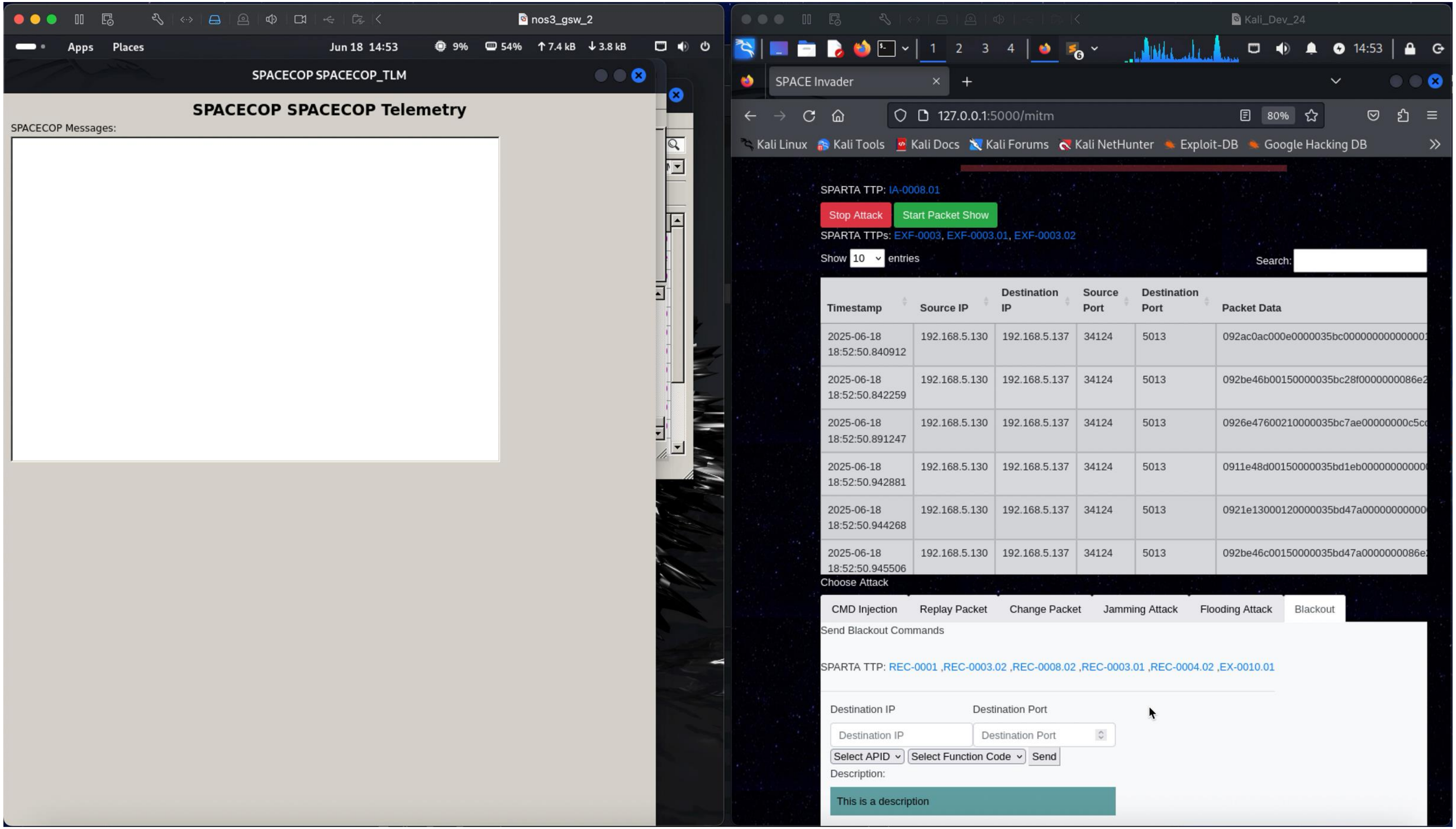
Index	Name	Value
0	PACKET_TIMESECONDS *	1712186649.545468
1	PACKET_TIMEFORMATTED *	2024/04/03 23:24:09.545
2	RECEIVED_TIMESECONDS *	1712186649.545468
3	RECEIVED_TIMEFORMATTED *	2024/04/03 23:24:09.545
4	RECEIVED_COUNT *	41
5	CCSDS_STREAMID	2248
6	CCSDS_SEQ_FLAGS	3
7	CCSDS_SEQ_COUNT	45
8	CCSDS_LENGTH	11
9	CCSDS_SECONDS	46
10	CCSDS_SUBSECS	3276
11	CCSDS_SPARE	0



```
EVS Port1 42/1/CAM 28: CAM child task initialization complet
EVS Port1 42/1/FM 89: Child Task initialization complete
EVS Port1 42/1/RW 1: GENERIC_RW App Initialized. Version 0.1
2000-001-00:00:00.65000 CFE_ES_Main: CFE_ES_Main entering AP
2000-001-00:00:00.65000 CFE_ES_Main: CFE_ES_Main entering OP
EVS Port1 42/1/CFE_TIME 21: Stop FLYWHEEL
EVS Port1 42/1/SC 73: RTS Number 001 Started
EVS Port1 42/1/SCH 21: Major Frame Sync too noisy (Slot 1).
ation.
EVS Port1 42/1/DS 35: APP STATE command: state = 1
EVS Port1 42/1/TO_LAB_APP 3: TO telemetry output enabled for
EVS Port1 42/1/SC 121: Enable RTS group: FirstID=3, LastID=6
EVS Port1 42/1/SAMPLE 11: SAMPLE: NOOP command received
EVS Port1 42/1/SAMPLE 13: SAMPLE: Enable command received
EVS Port1 42/1/SAMPLE 14: SAMPLE: Device enabled
EVS Port1 42/1/SC 86: RTS 001 Execution Completed
EVS Port1 42/1/LC 28: Set LC state command: new state = 1
EVS Port1 42/1/RADIO 31: GENERIC_RADIO: Request device HK re
```

https://github.com/nasa/nos3

SpaceCOP Detecting Rogue App and Ransomware



SPACECOP SPACECOP_TLM

SPACECOP SPACECOP Telemetry

SPACECOP Messages:

SPARTA TTP: IA-0008.01

Stop Attack | Start Packet Show

SPARTA TTPs: EXF-0003, EXF-0003.01, EXF-0003.02

Show 10 entries

Search:

Timestamp	Source IP	Destination IP	Source Port	Destination Port	Packet Data
2025-06-18 18:52:50.840912	192.168.5.130	192.168.5.137	34124	5013	092ac0ac000e0000035bc00000000000000001
2025-06-18 18:52:50.842259	192.168.5.130	192.168.5.137	34124	5013	092be46b00150000035bc28f0000000086e2
2025-06-18 18:52:50.891247	192.168.5.130	192.168.5.137	34124	5013	0926e47600210000035bc7ae00000000c5cc
2025-06-18 18:52:50.942881	192.168.5.130	192.168.5.137	34124	5013	0911e48d00150000035bd1eb000000000000
2025-06-18 18:52:50.944268	192.168.5.130	192.168.5.137	34124	5013	0921e13000120000035bd47a000000000000
2025-06-18 18:52:50.945506	192.168.5.130	192.168.5.137	34124	5013	092be46c00150000035bd47a0000000086e2

Choose Attack

Send Blackout Commands

SPARTA TTP: REC-0001 ,REC-0003.02 ,REC-0008.02 ,REC-0003.01 ,REC-0004.02 ,EX-0010.01

Destination IP: Destination IP

Destination Port: Destination Port

Select APID | Select Function Code | Send

Description:

This is a description

Detecting Onboard Malware, But it may be too late…

Detection ≠ Mitigation

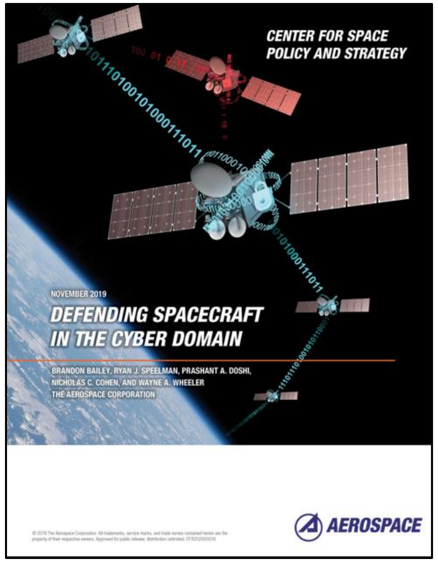
- As seen, SpaceCOP was able to detect the malware processes running, the files being modified and deleted, and system commands being executed
- However, the space operator may only be able to watch the alerts come down
  - Telemetry is only sent to the ground station when the spacecraft is within range
  - 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 **is essential**
  - 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

https://csps.aerospace.org/sites/default/files/2021-08/Bailey_DefendingSpacecraft_11052019.pdf



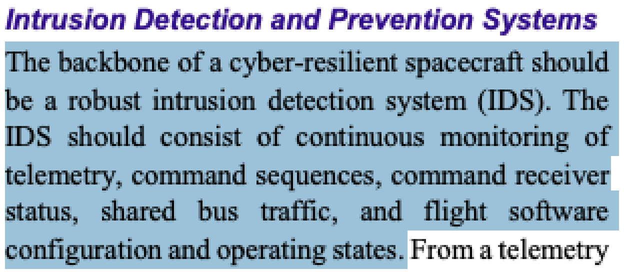
CENTER FOR SPACE POLICY AND STRATEGY

NOVEMBER 2019

DEFENDING SPACECRAFT IN THE CYBER DOMAIN

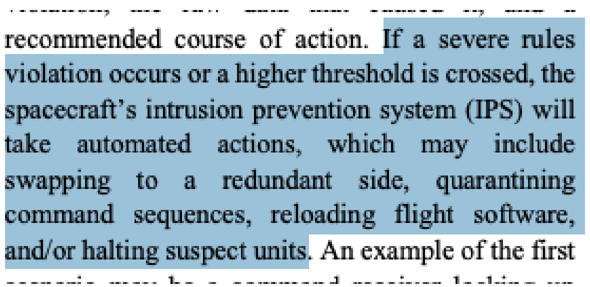
BRANDON BAILEY, RYAN J. SPEELMAN, PRASHANT A. DOSHI, NICHOLAS C. COHEN, AND WAYNE A. WHEELER
THE AEROSPACE CORPORATION

AEROSPACE

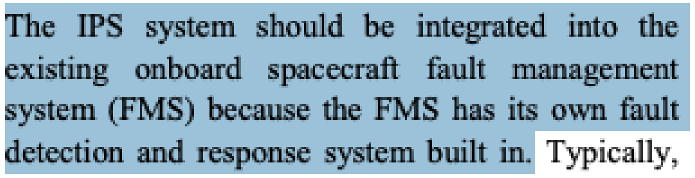


Intrusion Detection and Prevention Systems

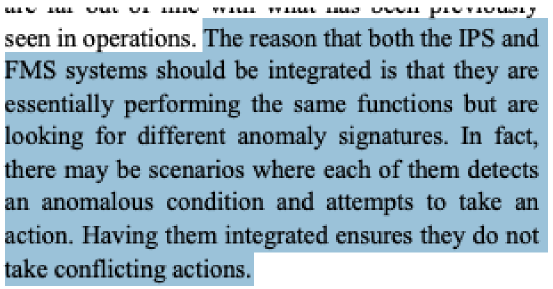
The backbone of a cyber-resilient spacecraft should be a robust intrusion detection system (IDS). The IDS should consist of continuous monitoring of telemetry, command sequences, command receiver status, shared bus traffic, and flight software configuration and operating states. From a telemetry



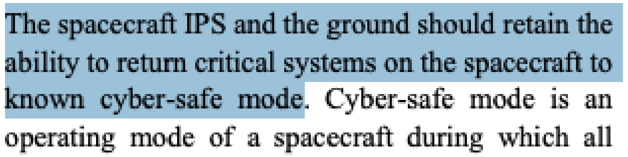
recommended course of action. If a severe rules violation occurs or a higher threshold is crossed, the spacecraft's intrusion prevention system (IPS) will take automated actions, which may include swapping to a redundant side, quarantining command sequences, reloading flight software, and/or halting suspect units. An example of the first



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,



are far out of line with what has been previously 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

- SPARTA techniques and now IOBs support this position that attacks can occur and be detected but response is needed to assure mission continuity

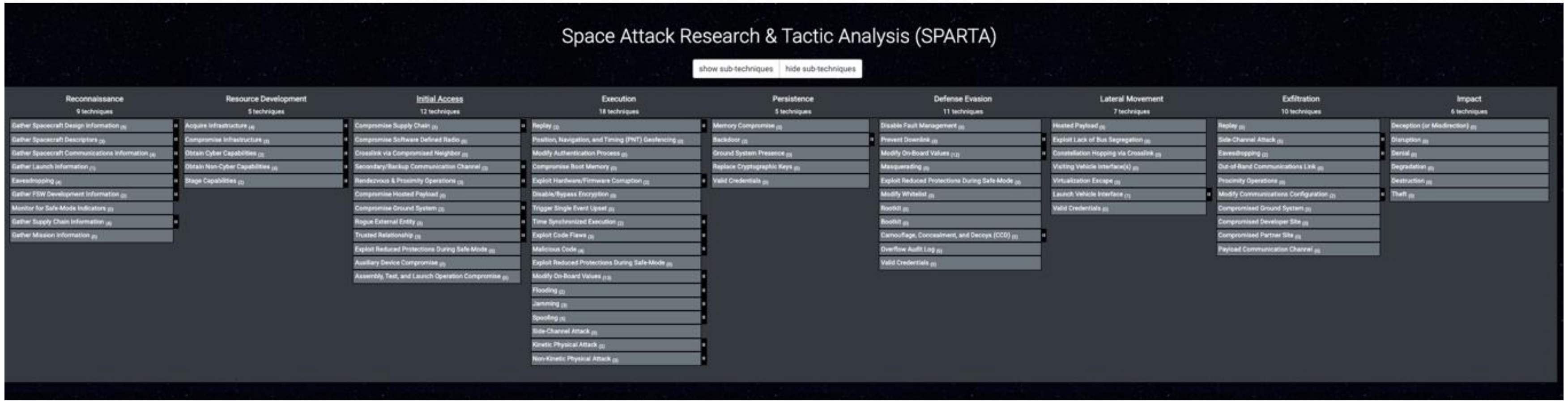
Detection and Response are Necessary, Cyber can be Mission Killer

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 mission-specific 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

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS



Space Attack Research & Tactic Analysis (SPARTA)

Reconnaissance 9 techniques	Resource Development 5 techniques	Initial Access 12 techniques	Execution 18 techniques	Persistence 5 techniques	Defense Evasion 11 techniques	Lateral Movement 7 techniques	Exfiltration 10 techniques	Impact 6 techniques
Gather Spacecraft Design Information	Acquire Infrastructure	Compromise Supply Chain	Replay	Memory Compromise	Disable Fault Management	Hosted Payload	Replay	Deception (or Misdirection)
Gather Spacecraft Descriptors	Compromise Infrastructure	Compromise Software Defined Radio	Position, Navigation, and Timing (PNT) Geofencing	Backdoor	Prevent Downlink	Exploit Lack of Bus Segregation	Side-Channel Attack	Disruption
Gather Spacecraft Communications Information	Obtain Cyber Capabilities	Crosslink via Compromised Neighbor	Modify Authentication Process	Ground System Presence	Modify On-Board Values (12)	Constellation Hopping via Crosslink	Eavesdropping	Denial
Gather Launch Information	Obtain Non-Cyber Capabilities	Secondary/Backup Communication Channel	Compromise Boot Memory	Replace Cryptographic Keys	Masquerading	Visiting Vehicle Interface(s)	Out-of-Band Communications Link	Degradation
Eavesdropping	Stage Capabilities	Rendezvous & Proximity Operations	Exploit Hardware/Firmware Corruption	Valid Credentials	Exploit Reduced Protections During Safe-Mode	Virtualization Escape	Proximity Operations	Destruction
Gather FSW Development Information		Compromise Hosted Payload	Disable/Bypass Encryption		Modify Whitelist	Launch Vehicle Interface	Modify Communications Configuration	Theft
Monitor for Safe-Mode Indicators		Compromise Ground System	Trigger Single Event Upset		Rootkit	Valid Credentials	Compromised Ground System	
Gather Supply Chain Information		Rogue External Entity	Time Synchronized Execution		Bootkit		Compromised Developer Site	
Gather Mission Information		Trusted Relationship	Exploit Code Flaws		Camouflage, Concealment, and Decoys (CCD)		Compromised Partner Site	
		Exploit Reduced Protections During Safe-Mode	Malicious Code		Overflow Audit Log		Payload Communication Channel	
		Auxiliary Device Compromise	Exploit Reduced Protections During Safe-Mode		Valid Credentials			
		Assembly, Test, and Launch Operation Compromise	Modify On-Board Values (12)					
			Flooding					
			Jamming					
			Spoofing					
			Side-Channel Attack					
			Kinetic Physical Attack					
			Non-Kinetic Physical Attack					

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
- Indicators of Behavior: https://sparta.aerospace.org/related-work/iob

Other Papers and Resources

CYSAT ’23: https://www.youtube.com/watch?v=I9nezXxO3iE
CYSAT ‘24: https://www.youtube.com/watch?v=jtMFI1DpAFo

- 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
  - DEF CON 2024: From Theory to Reality: Demonstrating the Simplicity of SPARTA Attacks
- 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
  - 2024: Space Segment Cybersecurity Profile
- 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