Space Attack Research & Tactic Analysis

Brandon Bailey, Brad Roeher, Randi Tinney
Cybersecurity and Advanced Platforms Subdivision (CAPS)
Cyber Assessment & Research Dept (CARD)
The Aerospace Corporation

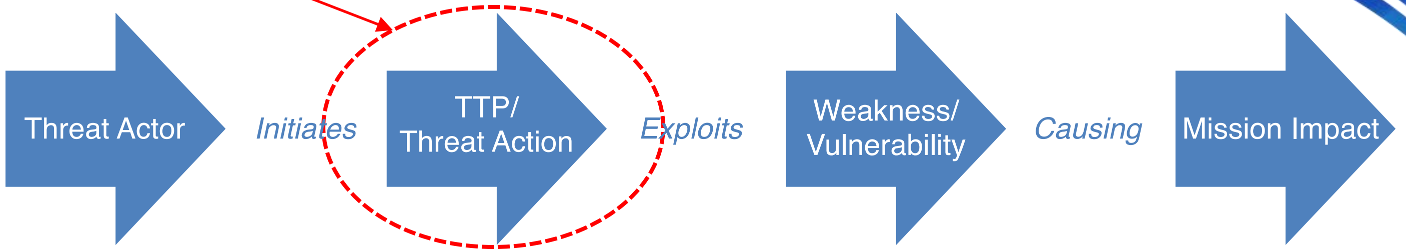
November 2022

brandon.bailey@aero.org
240.521.4326 (c)

Approved for public release. OTRs 2022-01250, 2022-00950, & 2023-00004

Problem Statement: Where are these documented for space and how do you mitigate?

Attacks/TTPs

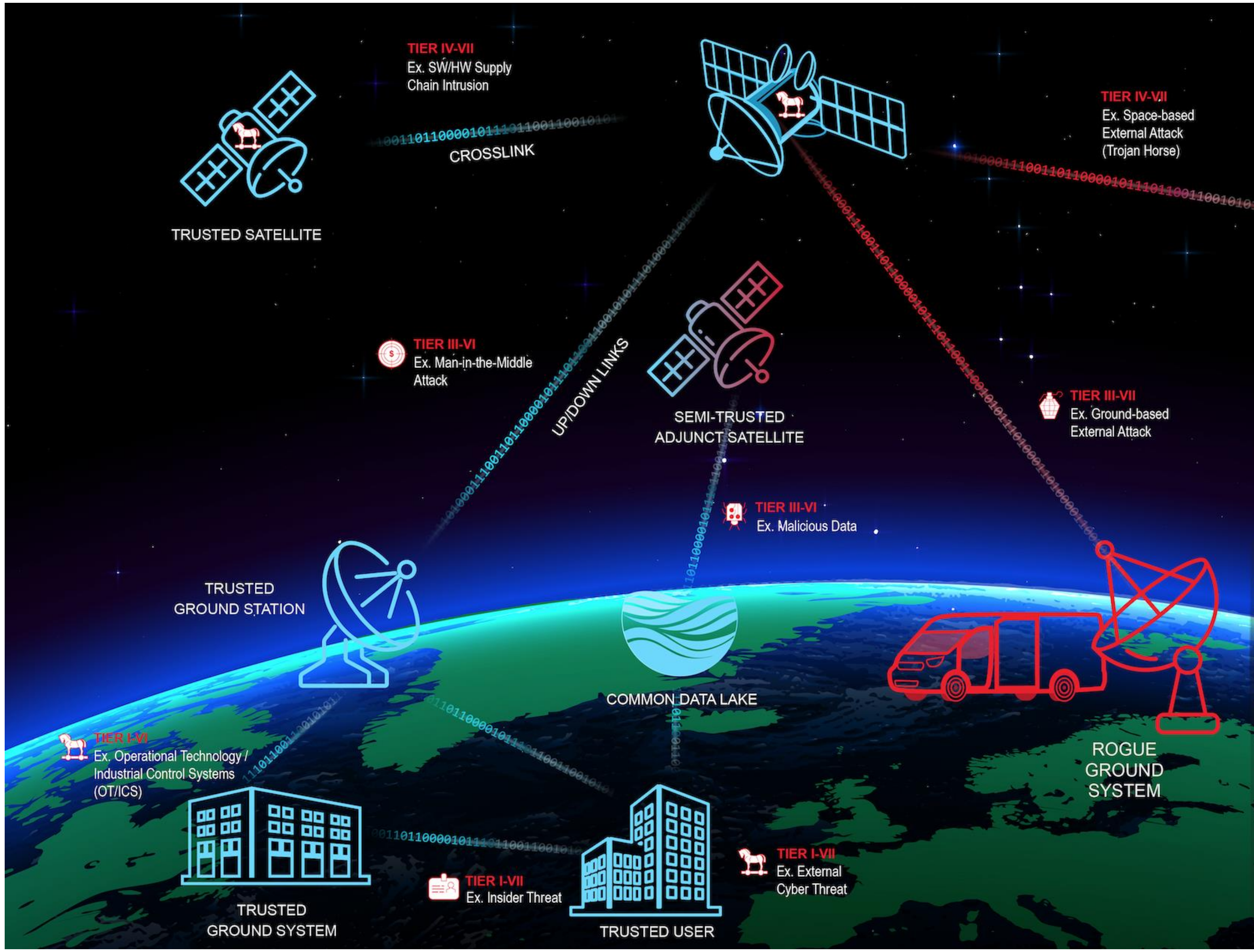


SPD-5[1] defines "Space System" as *"a combination of systems, to include ground systems, sensor networks, and one or more space vehicles, that provides a space-based service."*

SPD-5[1] states *Protection against unauthorized access to critical space vehicle functions. This should include safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures designed to remain secure against **existing** and **anticipated** threats during the entire mission lifetime*

Attacks / TTPs can occur across all segments within a space system {i.e., ground, link, and space} to achieve the desired impact for the threat actor

TTP= Tactics, Techniques, & Procedures



THREAT TIERS AND LEVELS OF SOPHISTICATION

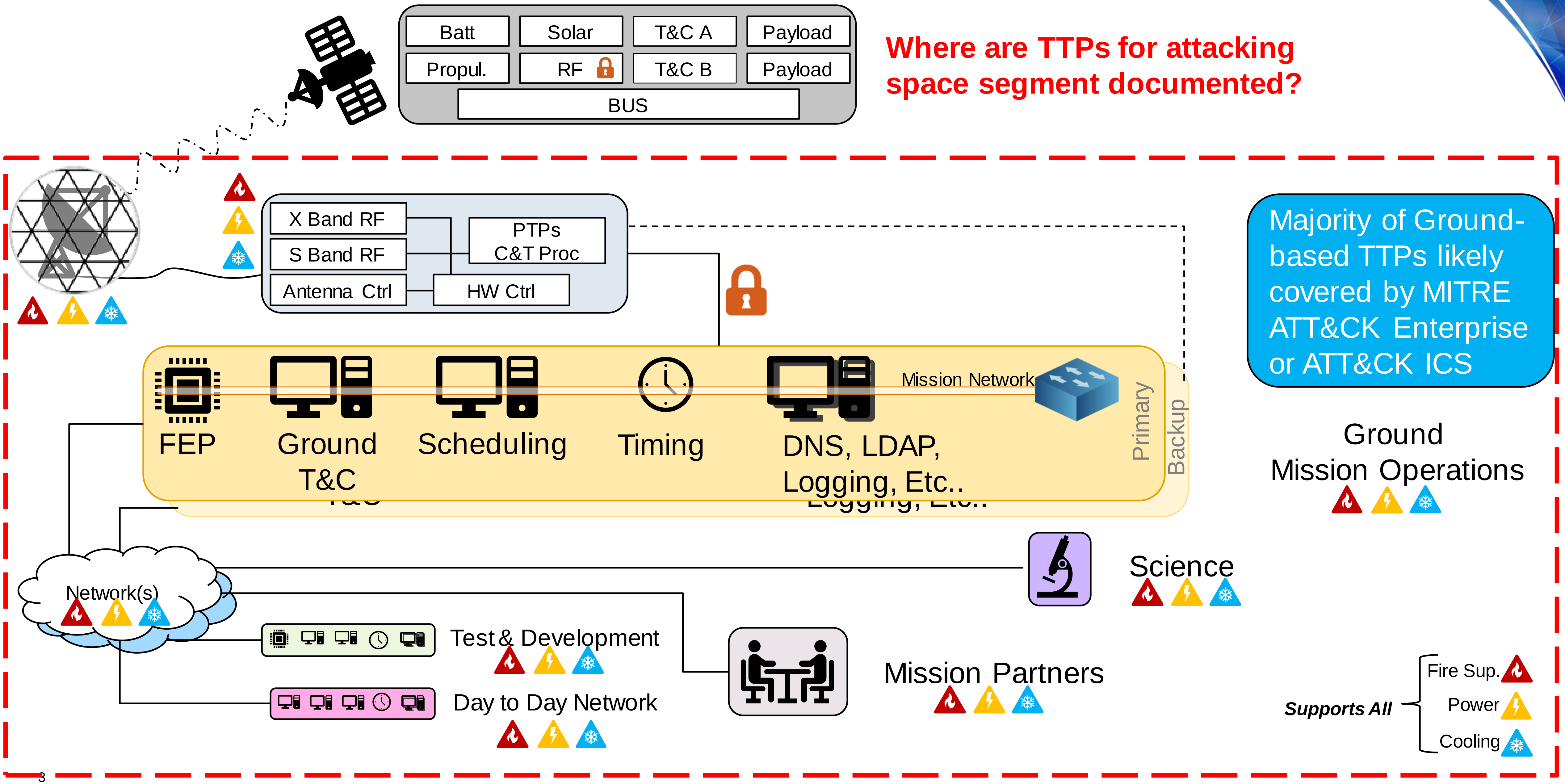
Tier	Category	Skills	Malice
Tier I:	Script kiddies	VERY LOW	LOW
Tier II:	Hackers for hire	LOW	MODERATE
Tier III:	Small hacker teams; non-state actors	MODERATE	MODERATE
Tier IV:	Insider threats (e.g. disgruntled employees)	LOW-HIGH	LOW-HIGH
Tier V:	Large, well organized teams; criminal; non-state, or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

1 Memorandum on Space Policy Directive – 5 Cybersecurity Principles for Space Systems, Sep 2020

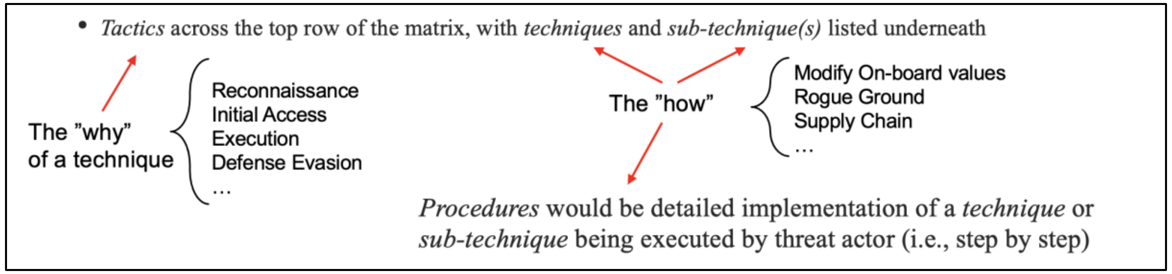
Space Systems – Large Attack Surface (IT,OT,SV)

Where are TTPs for attacking space segment documented?

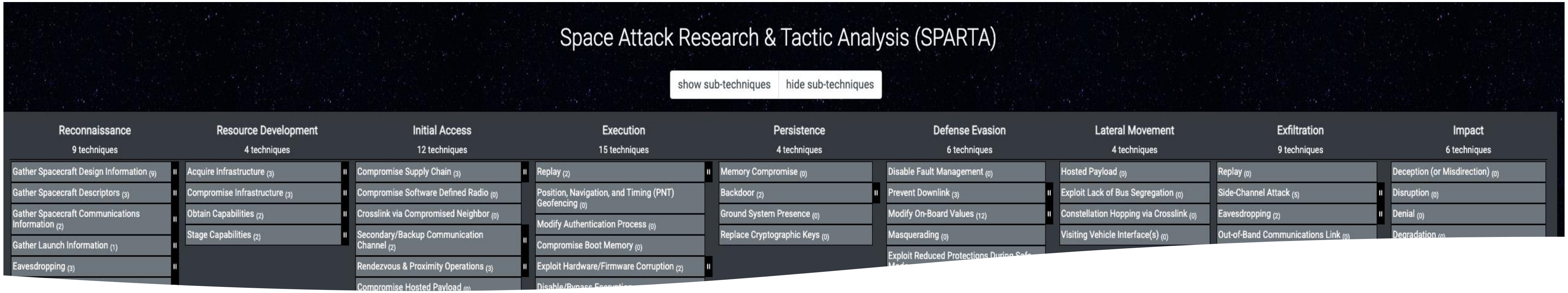


Space Attack Research & Tactic Analysis (SPARTA)

- 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*



- Aerospace's SPARTA matrix is the first-of-its-kind body of knowledge on cybersecurity protections for spacecraft and space systems, filling a critical vulnerability gap for the U.S. space enterprise



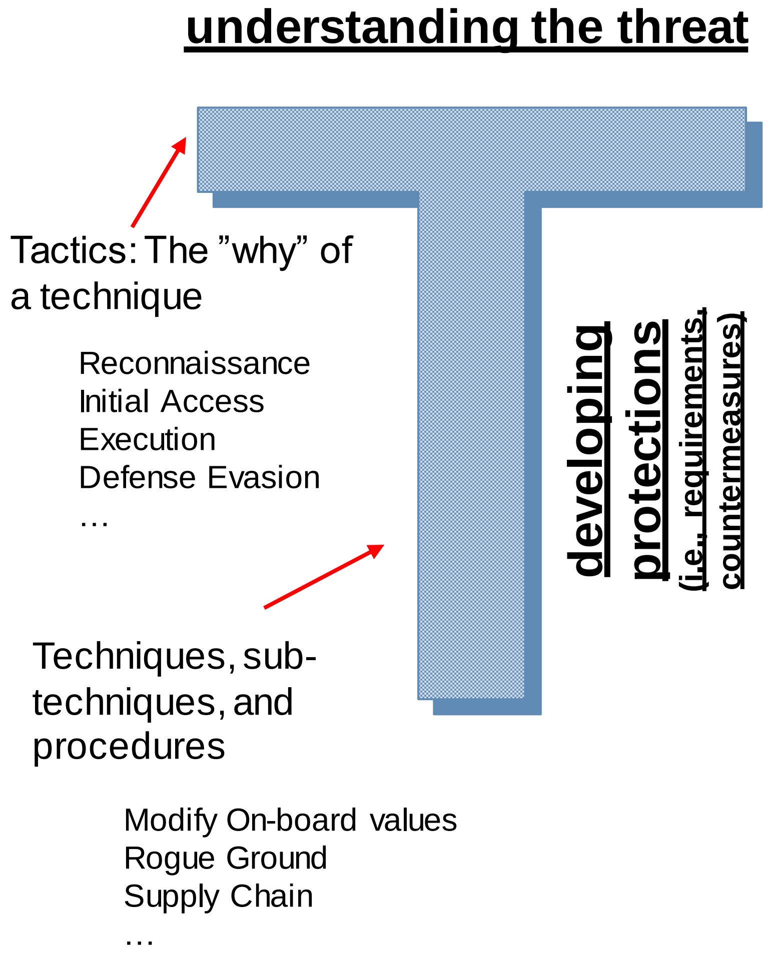
SPARTA provides unclassified information to space professionals about how spacecraft may be compromised

Space Attack Research & Tactic Analysis (SPARTA)

An evolution of Aerospace's technical insight in cybersecurity

- SPARTA has resulted from consistent technical insight from Aerospace's Cybersecurity and Advanced Platforms Subdivision (CAPS) across the space enterprise
  - 2019: Defending Spacecraft in the Cyber Domain (CSPS Paper)
  - 2020: Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices (published in response to SPD-5)
  - 2020 | 2021 : DefCon Talks at Aerospace Village
  - 2021: Cybersecurity Protections for Spacecraft: A Threat based Approach (release TOR 2021-01333 REV A)
  - 2022: Protecting Space Systems from Cyber Attack (Medium/1MSF)

- SPARTA leverages cybersecurity industry-standard approaches to communicate 3+ years of Aerospace's work to our customers on one of their hardest problems (cyber)



Enabling space enterprise resiliency through a wealth of cyber knowledge via a publicly releasable tool

SPARTA Use Cases

Let's Deep Dive on These Three Use Cases

- Space system developers
  - *Engineers now have a resource that contains TTPs, threats, and countermeasures to enable the engineering of protections early in the lifecycle -- establishing countermeasures to disrupt the attack chains*
- Defensive Cyber Operations
  - *Enables the building of monitoring solutions, analytics, automation, etc. for DCO Operators/Blue Team members*
    - Measure how effective systems/operators are at detecting TTPs for their specific space system
      - *Ex: These commands/telemetry possibly indicate TTP attacking the software watchdog timer {EX-0012.11}*
- Threat intelligence reporting / tracking of TTPs
  - *Report data to the community tying threat actor's TTPs against space systems using a common taxonomy*
    - Leverage the unique identifiers and aggregate reporting using a similar approach as the current industry standard for Enterprise IT systems
- Assessments / Table-Tops
  - *Provides a framework for assessment engineers / red teamers to leverage for designing attack chains against the space segment*
- Education / Training / Research
  - *Expands the footprint of knowledge to a wider audience – raises the bar on what is considered common knowledge*

SPARTA will crowdsource info from space enterprise researchers and threat intel via sparta@aero.org

Use Case Example

Space System Developers

Space System Developers

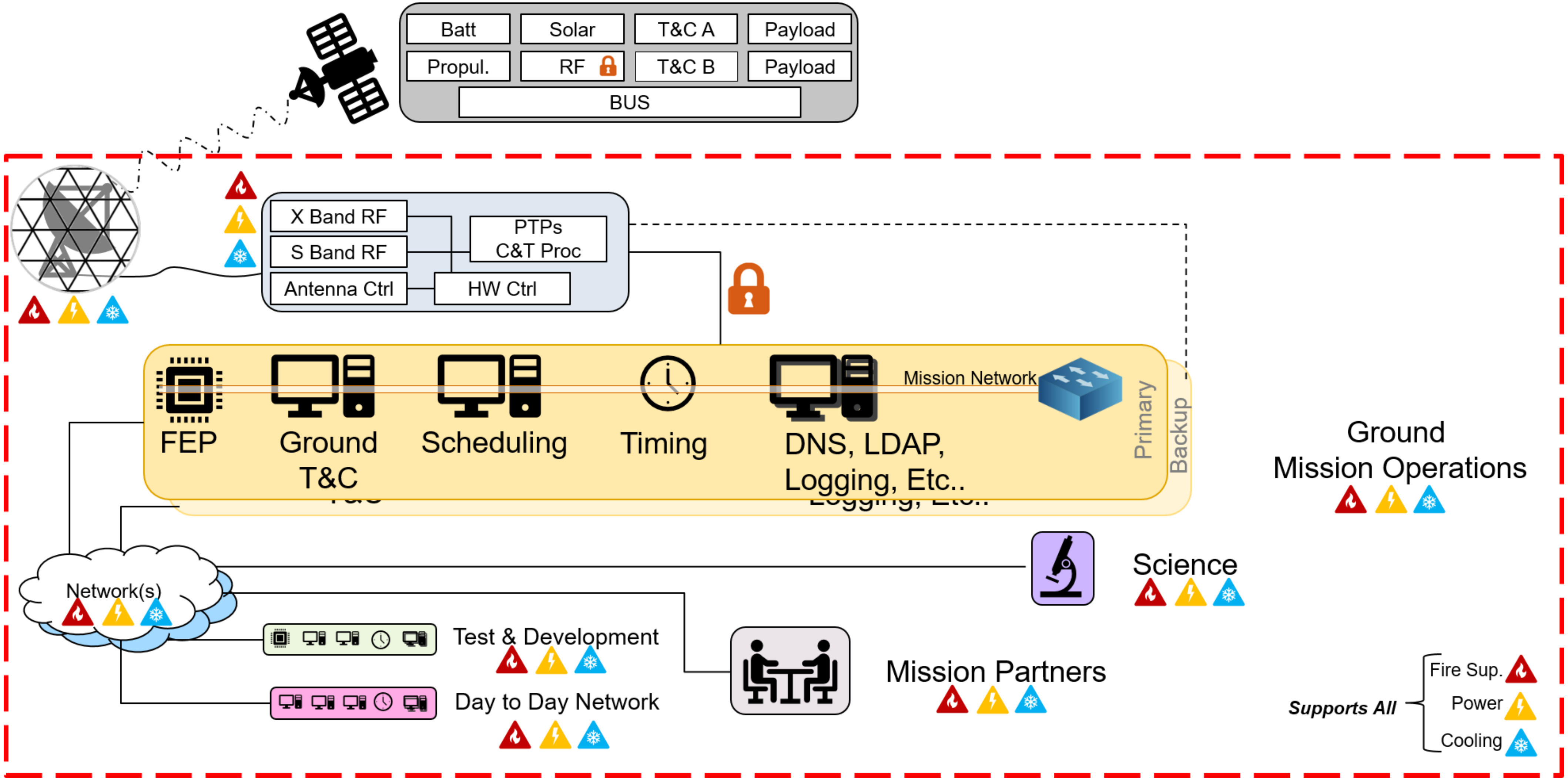
Engineers now have a resource that contains TTPs, threats, and countermeasures to enable the engineering of protections early in the lifecycle -- establishing countermeasures to disrupt the attack chains

- Step 1: Enumerate end-to-end system during all phases of mission development and operations
- Step 2: Review each threat, technique and sub-technique and make applicability determination based on your specific mission/system context FOR EACH element identified in Step 1
  - *Techniques mapped to Aerospace Threat IDs can assist with generating requirement language*
- Step 3: Evaluate current design choices to identify potential gaps that would leave element(s) vulnerable to applicable threats/techniques (as determined in Step 2)
  - *Consider implementing SPARTA Countermeasures (CM) mapped to applicable techniques where gaps exist in current design*
    - Implementing multiple countermeasures aligns with defense-in-depth principles published in related work area of SPARTA - https://sparta.aerospace.org/related-work/did-space and TOR 2021-01333 REV A
  - *Countermeasures in SPARTA can help system developers document defensive capability statements and can be a bridge to NIST control compliance as they are mapped to 800-53 Rev 5*
    - Many space system developers find it difficult to translate NIST guidance into spacecraft implementation

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

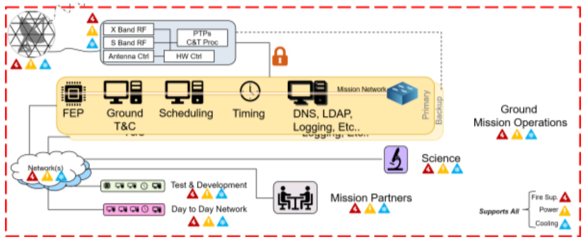
Space System Developers

- **Step 1: Enumerate <u>end-to-end</u> system during all phases of mission development and operations**

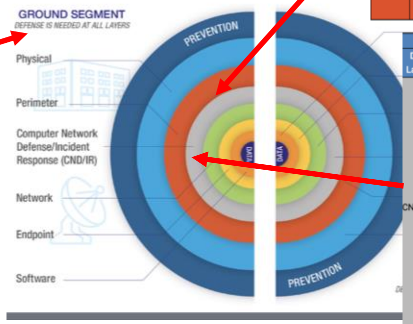


Space System Developers

Step 2 – Ground System

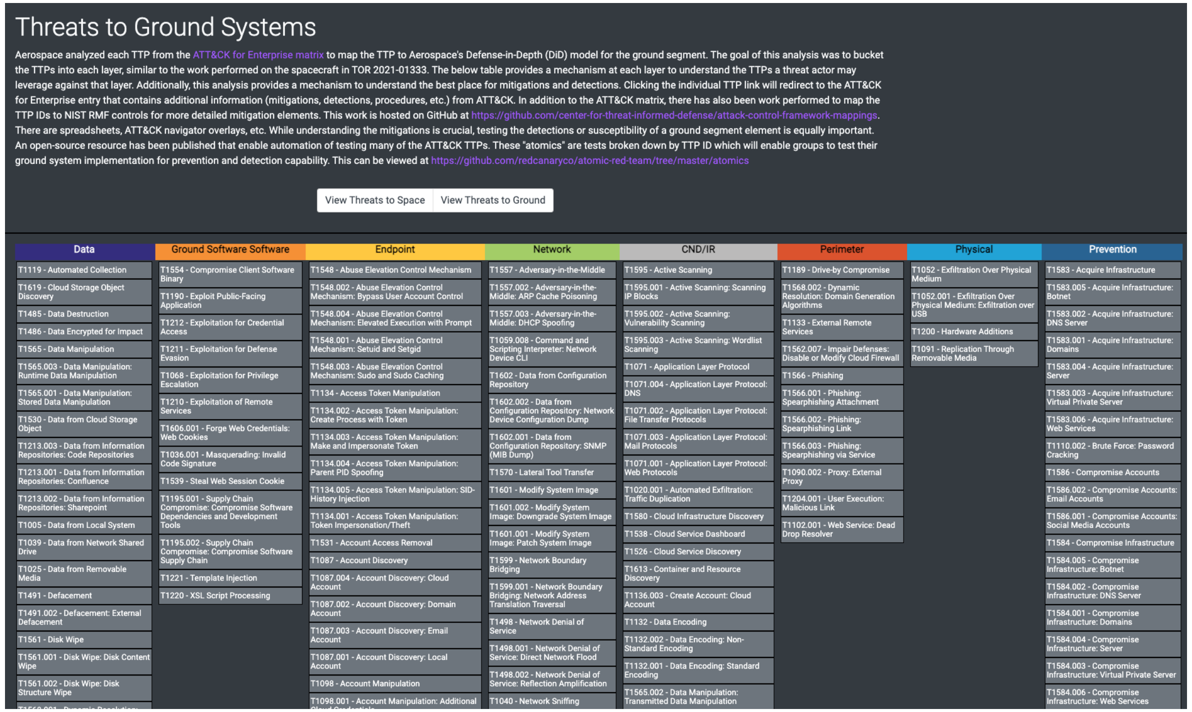


- A combination of Enterprise IT and ICS/OT cyber controls/protections would be applied to the systems enumerated on ground using any of the following resources
  - https://sparta.aerospace.org/related-work/did-space
  - https://sparta.aerospace.org/countermeasures/CM0005
  - https://sparta.aerospace.org/related-work/threats/ground



Ground Segment		
DiD Layer	DiD Sub-Layer	Implementation Goal
Perimeter	Virtual Private Network (VPN)/Remote Access	VPN, multi-factor authentication, and host verification required for access to internal system resources.
	Data Loss Prevention (DLP)	DLP policy/solution is secure and efficient.
	Demilitarized Zones (DMZs)/Securiy Zones	Services hosted for external consumption are properly protected by DMZ/security zoning AND proper limitations placed on internal network access and authentication.
	Firewall	Firewalls are configured with highly refined rulesets AND firewall configurations are routinely verified AND firewall configurations are routinely verified

Ground Segment		
DiD Layer	DiD Sub-Layer	Implementation Goal
CND/IR	Forensics	Has dedicated forensics capability and personnel.
	Hunting	Personnel are trained and tasked to continuously monitor logs/traffic.
	Threat Intelligence	Collaborates with threat intelligence sources both internal and external to the organization and integrates into tools where appropriate
	IDS/IPS	IDS/IPS has insight to all critical areas of network AND staff is in place to monitor alerts 24/7.
	Incident Response Policy/Procedures	Has fully documents IR procedures. AND performs self-assessments via tabletop exercies.
	Sensors	Sensors are deployed in-line to monitor critical data flows OR sensors are place at aggregation points.
	Security Information & Event Manager (SIEM)	SIEM is present in and customized alerts are configured. AND performs 24/7 monitoring of events (on-site or remote alerting).
	Security Operations Center (SOC)	Has a local dedicated SOC with insight into all the necessary critical data flows.
	Test Access Points (TAPs)	Full deployment of TAPs in-line of all critical data flows OR TAPs are deployed in an aggregation style deployment where all critical data flows are captured.



CM0005	Ground-based Countermeasures	This countermeasure is focused on the protection of terrestrial assets like ground networks and development environments/contractor networks, etc. Traditional detection technologies and capabilities would be applicable here. Utilizing resources from NIST CSF to properly secure these environments using identify, protect, detect, recover, and respond is likely warranted. Additionally, NISTIR 8401 may provide resources as well since it was developed to focus on ground-based security for space systems (https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.pdf). Furthermore, the MITRE ATT&CK framework provides IT focused TTPs and their mitigations https://attack.mitre.org/mitigations/enterprise/. Several recommended NIST 800-53 Rev5 controls are provided for reference when designing ground systems/networks.	AC-1 | AC-10 | AC-11 | AC-11(1) | AC-12 | AC-12(1) | AC-14 | AC-16 | AC-16(6) | AC-17 | AC-17(1) | AC-17(10) | AC-17(2) | AC-17(3) | AC-17(4) | AC-17(6) | AC-17(9) | AC-18 | AC-18(1) | AC-18(3) | AC-18(4) | AC-18(5) | AC-19 | AC-19(5) | AC-2 | AC-2(1) | AC-2(11) | AC-2(12) | AC-2(13) | AC-2(2) | AC-2(3) | AC-2(4) | AC-2(9) | AC-20 | AC-20(1) | AC-20(2) | AC-20(3) | AC-20(5) | AC-21 | AC-22 | AC-3 | AC-3(11) | AC-3(13) | AC-3(15) | AC-3(4) | AC-4 | AC-4(23) | AC-4(24) | AC-4(25) | AC-4(26) | AC-4(31) | AC-4(32) | AC-6 | AC-6(1) | AC-6(10) | AC-6(2) | AC-6(3) | AC-6(5) | AC-6(8) | AC-6(9) | AC-7 | AC-8 | AT-2(4) | AT-2(4) | AT-2(5) | AT-2(6) | AT-3 | AT-3(2) | AT-4 | AU-10 |

. . .

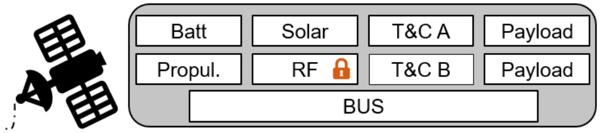
Targeted analysis of NIST Rev 5 controls important for ground systems

NIST to TTP Mappings - https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings

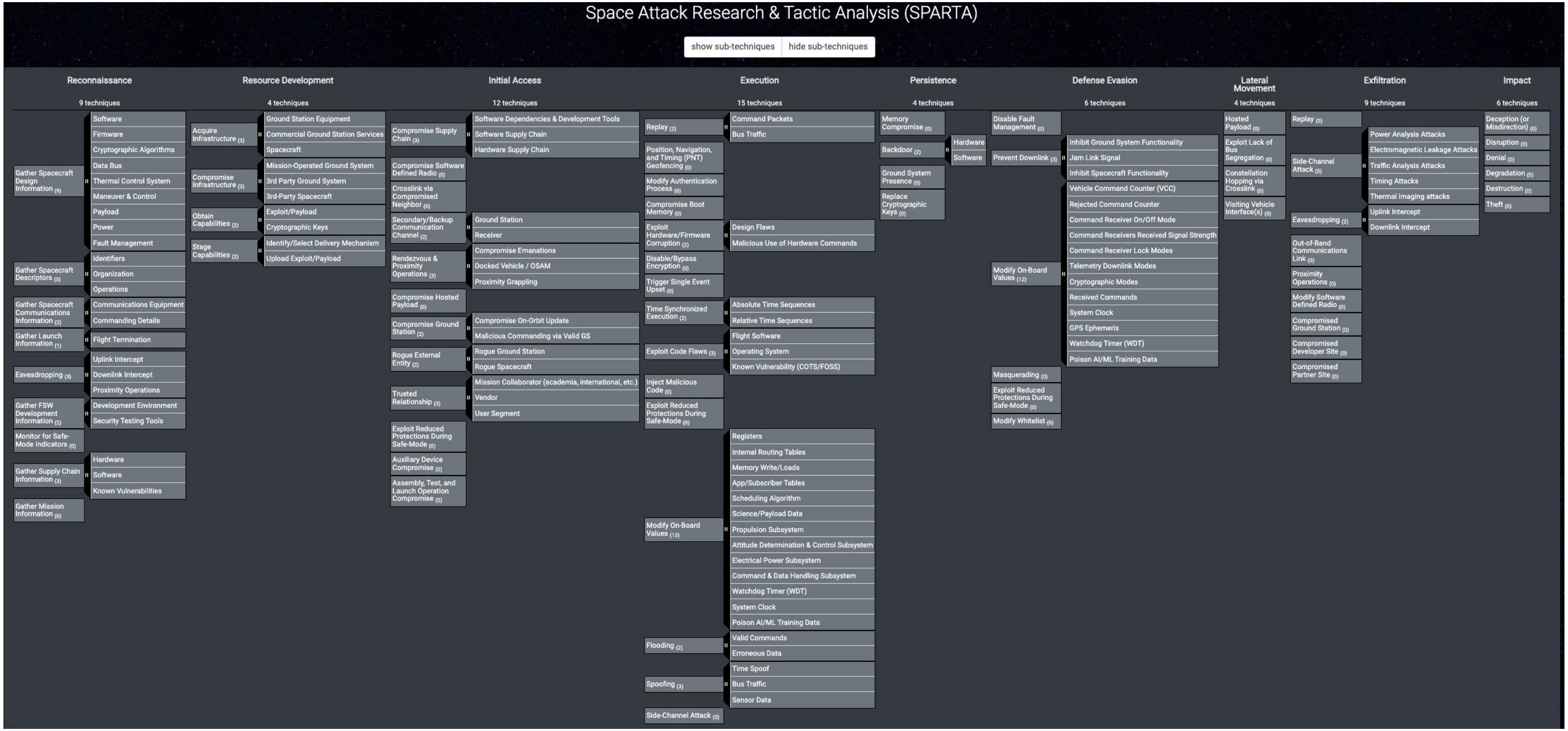
Automated Ground-based Tests per TTP - https://github.com/redcanaryco/atomic-red-team/tree/master/atomics

Space System Developers

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS



- **Step 2:** Review each SPARTA technique/sub-technique and determine applicability based on specific mission/system context for each SPACE SEGMENT element identified in Step 1



SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Space System Developers

- **Step 2 (*cont.*):** Techniques mapped to Aerospace Threat IDs can assist with generating requirement language.

Compromise Boot Memory

Threat actors may manipulate boot memory in order to execute malicious code, bypass internal processes, or DoS the system. This technique can be used to perform other tactics such as Defense Evasion.

ID: EX-0004
Sub-techniques: No sub-techniques
Related Aerospace Threat IDs: SV-IT-3 | SV-SP-4
Related MITRE ATT&CK TTPs: T1495 | T1601 | T1542 | T1553 | T1195
Tactic: Execution
Created: 2022/10/19
Last Modified: 2022/10/19

The spacecraft shall perform attestation at each stage of startup and ensure overall trusted boot regime (i.e., root of trust). {SV-IT-3} {SI-7(9)}	The spacecraft shall allocate enough SRAM memory for secure boot firmware execution. {SV-IT-3} {SI-7(9)}
The trusted boot/RoT shall be a separate compute engine controlling the trusted computing platform cryptographic processor. {SV-IT-3} {SI-7(9)}	The spacecraft secure boot mechanism shall be Commercial National Security Algorithm Suite (CNSA) compliant. {SV-IT-3} {SI-7(9)}
The trusted boot/RoT computing module shall be implemented on radiation tolerant burn-in (non-programmable) equipment. {SV-IT-3} {SI-7(9)}	The spacecraft shall support the algorithmic construct Elliptic Curve Digital Signature Algorithm (ECDSA) NIST P-384 + SHA-38{SV-IT-3} {SI-7(9)}
The spacecraft boot firmware must verify a trust chain that extends through the hardware root of trust, boot loader, boot configuration file, and operating system image, in that order. {SV-IT-3} {SI-7(9)}	The spacecraft hardware root of trust must be an ECDSA NIST P-384 public key. {SV-IT-3} {SI-7(9)}
The spacecraft boot firmware must enter a recovery routine upon failing to verify signed data in the trust chain, and not execute or trust that signed data. {SV-IT-3} {SI-7(9)}	The spacecraft hardware root of trust must be loadable only once, post-purchase. {SV-IT-3} {SI-7(9)}
The spacecraft shall allocate enough boot ROM memory for secure boot firmware execution. {SV-IT-3} {SI-7(9)}	The spacecraft boot firmware must validate the boot loader, boot configuration file, and operating system image, in that order, against their respective signatures. {SV-IT-3} {SI-7(9)}

Space System Developers

- **Step 3**: Evaluate current design choices to identify potential gaps that would leave element(s) vulnerable to applicable techniques (as determined in Step 2). Consider implementing SPARTA Countermeasures (CM) mapped to applicable techniques where gaps exist in current design.

Compromise Boot Memory

Threat actors may manipulate boot memory in order to execute malicious code, bypass internal processes, or DoS the system. This technique can be used to perform other tactics such as Defense Evasion.

Countermeasures

ID	Name	Description
CM0028	Tamper Protection	Perform physical inspection of hardware to look for potential tampering. Leverage tamper proof protection where possible when shipping/receiving equipment.
CM0015	Software Source Control	Prohibit the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code.
CM0018	Dynamic Analysis	Employ dynamic analysis (e.g., using simulation, penetration testing, fuzzing, etc.) to identify software/firmware weaknesses and vulnerabilities in developed and incorporated code (open source, commercial, or third-party developed code). Testing should occur (1) on potential system elements before acceptance; (2) as a realistic simulation of known adversary tactics, techniques, procedures (TTPs), and tools; and (3) throughout the lifecycle on physical and logical systems, elements, and processes.
CM0021	Software Digital Signature	Prevent the installation of Flight Software without verification that the component has been digitally signed using a certificate that is recognized and approved by the mission.
CM0023	Configuration Management	Use automated mechanisms to maintain and validate baseline configuration to ensure the spacecraft's is up-to-date, complete, accurate, and readily available.
CM0014	Secure boot	Software/Firmware must verify a trust chain that extends through the hardware root of trust, boot loader, boot configuration file, and operating system image, in that order. The trusted boot/RoT computing module should be implemented on radiation tolerant burn-in (non-programmable) equipment.

CM can help system developers document defensive capability statements and can be a bridge to NIST control compliance as they are mapped to 800-53 Rev 5

Technique-relevant CM are displayed on the respective technique pages, but the comprehensive list of CM can also be viewed independently.

Use Case Example

Threat Intel Reporting & Sharing

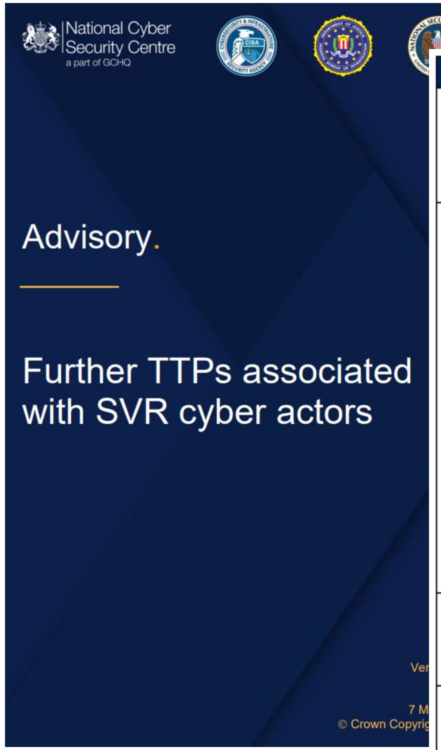
Threat Intel Reporting & Sharing

- Report data to the community tying threat actor's TTPs against space systems using a common taxonomy
  - Leverage the unique identifiers and aggregate reporting using a similar approach as the current industry standard for Enterprise IT systems

Table 1: Common Tactics and Techniques Employed by Russian State-Sponsored APT Actors

Tactic	Technique	Procedure
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Russian state-sponsored APT actors have performed large-scale scans in an attempt to find vulnerable servers.
	Phishing for Information [T1598]	Russian state-sponsored APT actors have conducted spearphishing campaigns to gain credentials of target networks.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Russian state-sponsored APT actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Russian state-sponsored APT actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.
	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	Russian state-sponsored APT actors have gained initial access to victim organizations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Russian state-sponsored APT actors have used `cmd.exe` to execute commands on remote machines. They have also used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands.
Persistence [TA0003]	Valid Accounts [T1078]	Russian state-sponsored APT actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.

https://www.cisa.gov/uscert/ncas/alerts/aa22-011a



Tactic	Technique	Procedure
Reconnaissance	T1595.002: Active Scanning	SVR frequently scans for publicly available exploits, most recently including Microsoft Exchange servers vulnerable to CVE-2021-26855.
Initial Access	T1190: Exploit Public-Facing Application	SVR frequently uses publicly available exploits to conduct widespread exploitation of vulnerable systems, including against Citrix, Pulse Secure, FortiGate, Zimbra and VMWare.
	T1195.002: Supply Chain Compromise: Compromise Software Supply Chain	SVR target organisations who supply privileged software to intelligence targets.
	T1199: Trusted Relationship	SVR leveraged access gained from the SolarWinds campaign to compromise a certificate issued by Mimecast, which it then used to authenticate a subset of Mimecast's products with customer systems.
Execution	T1059.005: Command and Scripting Interpreter: Visual Basic	SVR deployed Sibot, a simple custom downloader written in VBS, after compromising victims via SolarWinds.
Persistence	T1505.003: Server Software Component: Web Shell	SVR typically deploy a web shell on Microsoft Exchange servers following successful compromise.
	T1078: Valid Accounts	SVR actors have maintained persistence on high value targets using stolen credentials.

https://www.ncsc.gov.uk/news/joint-advisory-further-ttps-associated-with-svr-cyber-actors

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Threat Intel Reporting & Sharing

DefCon 2020 – Exploiting Spacecraft Example (https://www.youtube.com/watch?v=b8QWNiqTx1c)

Attacker performs a man-in-the-middle attack at the ground station where they record command packets in the UDP traffic for replaying to the spacecraft. In this example UDP mimics the radio frequency link. This same attack could be applied through RF signal sniffing vice UDP captures. From the spacecraft perspective, the flight software processes the traffic whether or not the traffic is coded to radio frequency signals and then decoded on the spacecraft. Upon receiving commands, the spacecraft flight software responds by downlinking command counter data to the ground indicating that commands were received. In this scenario, the attacker collected the commands at the ground station and then promptly replay the traffic to the spacecraft thereby causing the flight software to reprocess the commands again. This would be visible in the downlinked command counters and unless the ground operators are monitoring specific telemetry points, this attack would likely go unnoticed. If the replayed commands were considered critical commands like firing thrusters, then more critical impact on the spacecraft could be encountered.

Narrative structure hard to maintain consistently among individual reporters, let alone across multiple teams, organizations, or international partners

Makes communicating TTPs difficult and makes archiving historical attack data extremely burdensome on the industry

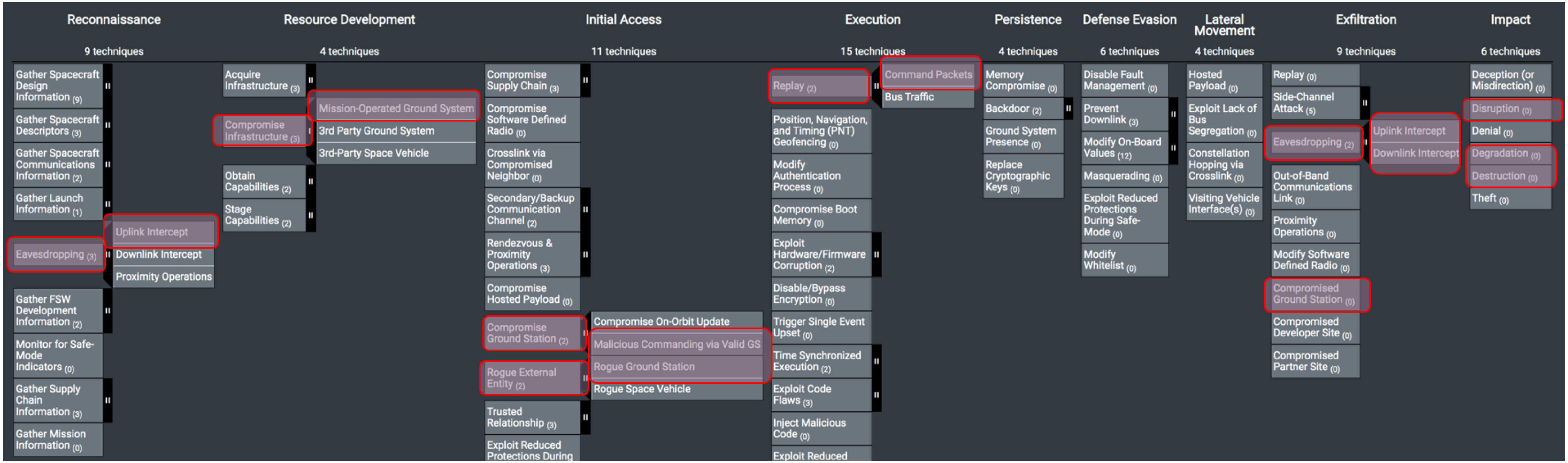
SPARTA can be used to characterize incidents (past, present, and future) at a more granular technical level by translating natural language reports into specific TTPs that can support countermeasure selection and implementation.

Next slide shows same example using SPARTA…

Threat Intel Reporting & Sharing

DefCon 2020 – Exploiting Spacecraft Example (https://www.youtube.com/watch?v=b8QWNiqTx1c)

Attacker performs a man-in-the-middle attack at the ground station where they record command packets in the UDP traffic [REC-0005 , RD-0005.01] for replaying to the spacecraft [EX-0001.01]. In this example UDP mimics the radio frequency link. This same attack could be applied through RF signal sniffing [REC-0005.01, IA-0008.01] vice UDP captures. From the spacecraft perspective, the flight software processes the traffic whether or not the traffic is coded to radio frequency signals and then decoded on the spacecraft. Upon receiving commands, the spacecraft flight software responds by downlinking command counter data to the ground indicating that commands were received [EXF-0003.02]. In this scenario, the attacker collected the commands at the ground station [EXF-0003.01, EXF-0007] and then promptly replay the traffic to the spacecraft [EX-0001.01] thereby causing the flight software to reprocess the commands again [EX-0001]. This would be visible in the downlinked command counters [REC-0005.02, EXF-0003.02] and unless the ground operators are monitoring specific telemetry points, this attack would likely go unnoticed. If the replayed commands were considered critical commands like firing thrusters, then more critical impact on the spacecraft could be encountered [IMP-0002, IMP-0004, IMP-0005].

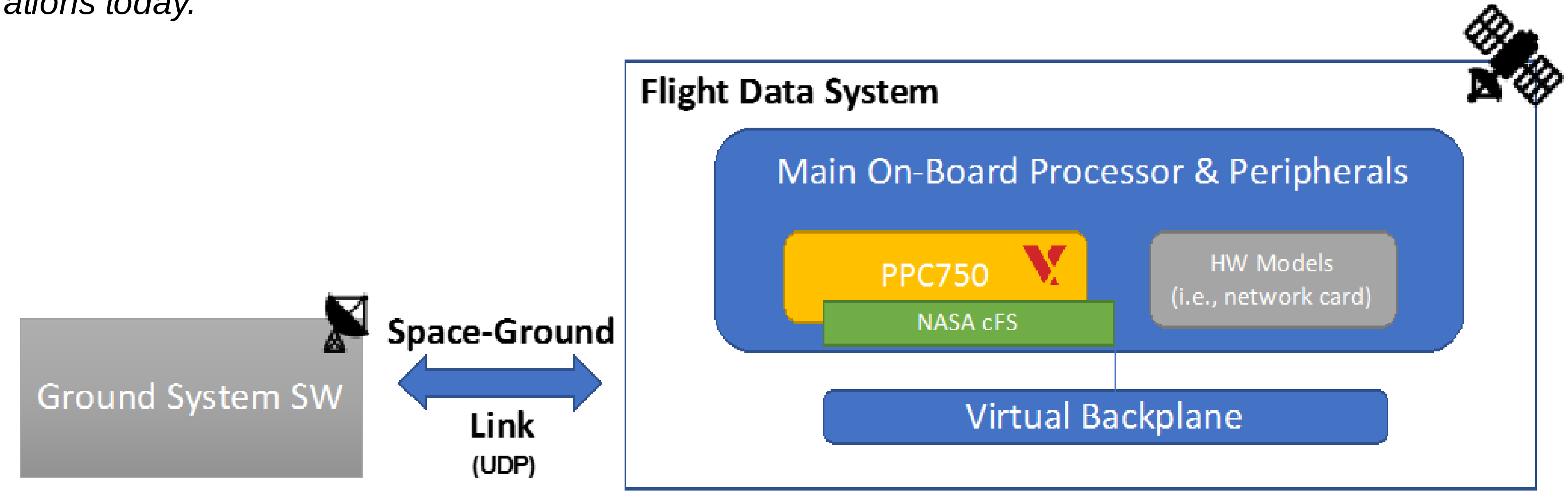


Threat Intel Reporting & Sharing

DefCon 2022 - Memory Manipulation Attack

Test Environment

- Leveraging a digital twin simulation capability at the Aerospace Corporation, a memory manipulation attack scenario was performed.
- The simulation environment in use and depicted below contains ground software that comes packaged with a front-end processor capability that "encodes/decodes" the messages to the spacecraft.
  - *This specific digital twin leverages VxWorks and PowerPC 750, which are widely used in space systems in operations today.*



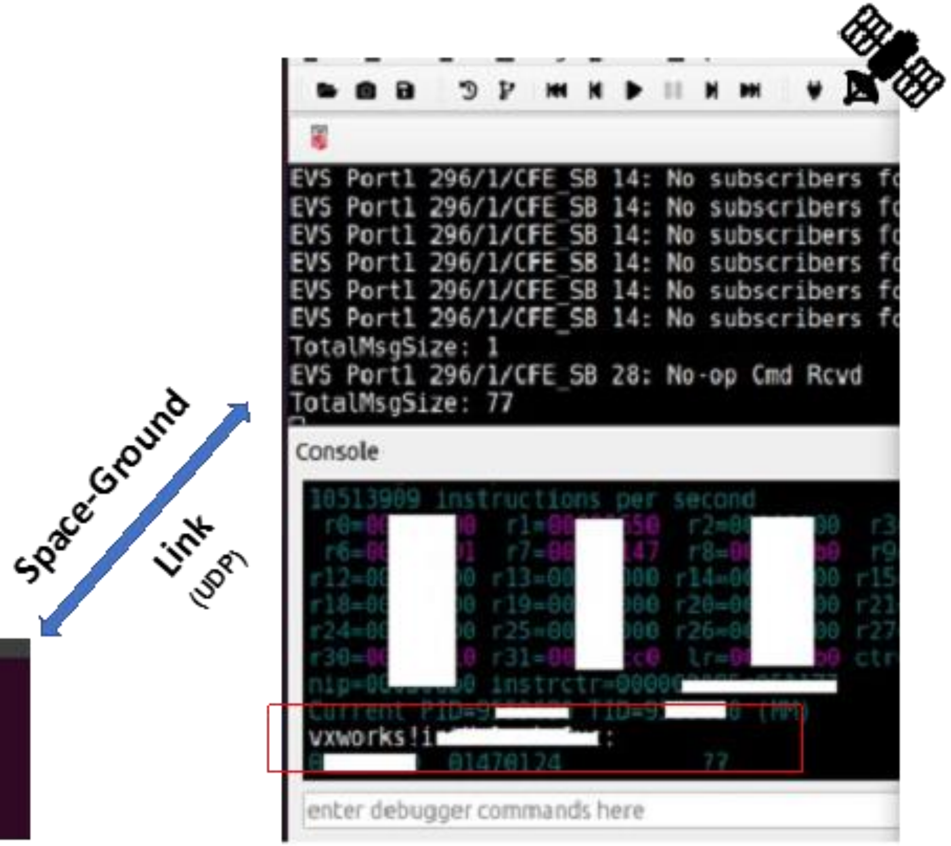
Threat Intel Reporting & Sharing

DefCon 2022 - Memory Manipulation Attack

Launching the Attack

This example requires significant effort in the reconnaissance phase [REC-0001, REC-0003] to understand the specific attack vectors. However, after understanding the memory maps/locations and how the VxWorks and PowerPC interrelates, the attack can be performed to disrupt [IMP-0002] and deny [IMP-0003] the spacecraft's ability to process information. Upon performing all the necessary research, a single command packet is all that is required to affect the spacecraft. Understanding the precise memory location and overwriting it with desired values, exploits the inherit trust between the ground and the spacecraft [IA-0009].

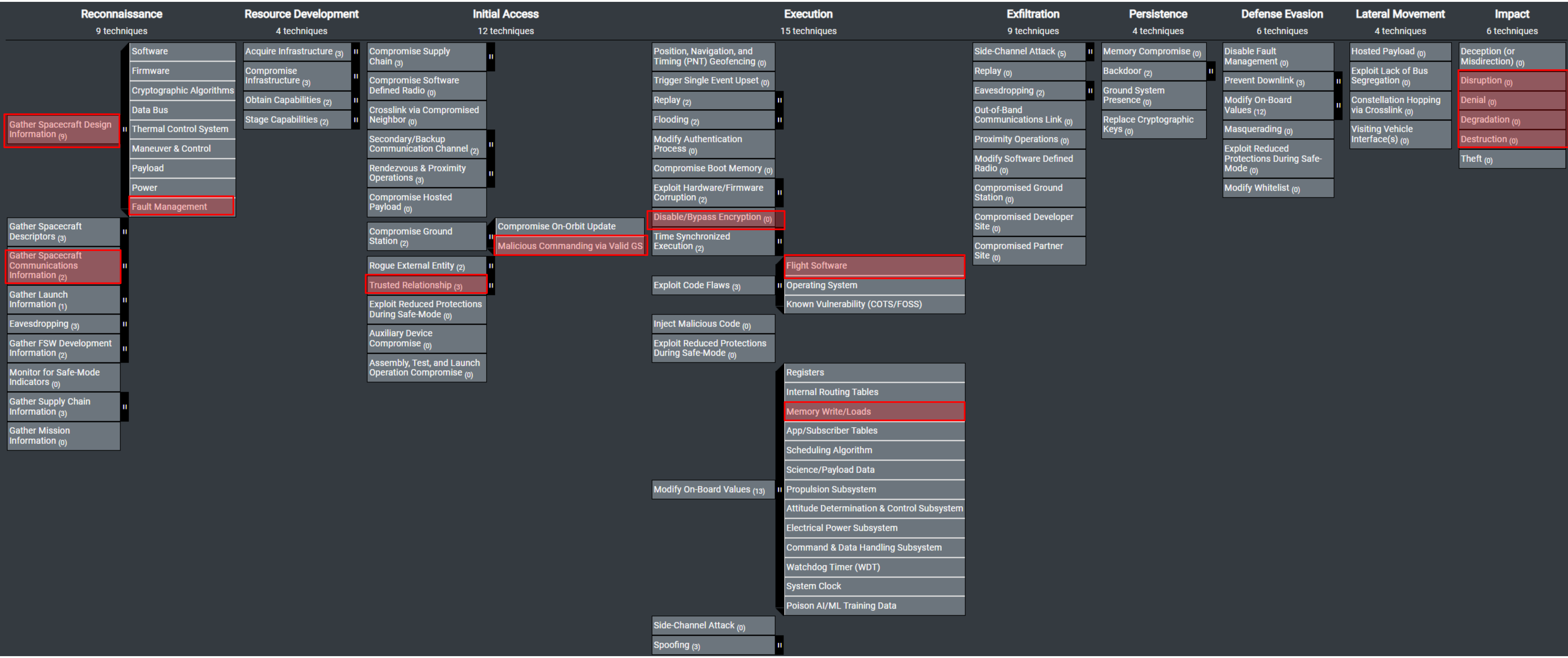
In this exploit example, the attacker leverages the authenticated/encrypted command pathway to send two commands to the spacecraft [IA-0007.02, EX-0006]. A simple NO-OP for demonstration purposes followed by a "magic packet" or "kill-pill" that corrupts the running state of the PowerPC processor thereby disabling the spacecraft's ability to process information. The below figure shows redacted information to remove the actual corrupting content, but the "vxworks!" is essentially the kernel throwing a panic and crashing. This is where having direct memory access [EX-0012.03] via the spacecraft flight software can be dangerous and must be protected [EX-0009.01]. There are many instances where the ground can issue legitimate commands to degrade/deny/destroy [IMP-0004, IMP-0003, IMP-0005] the spacecraft which puts pressure on fault management to account for this truth [REC-0001.09].



Threat Intel Reporting & Sharing

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

DefCon 2022 - Memory Manipulation Attack

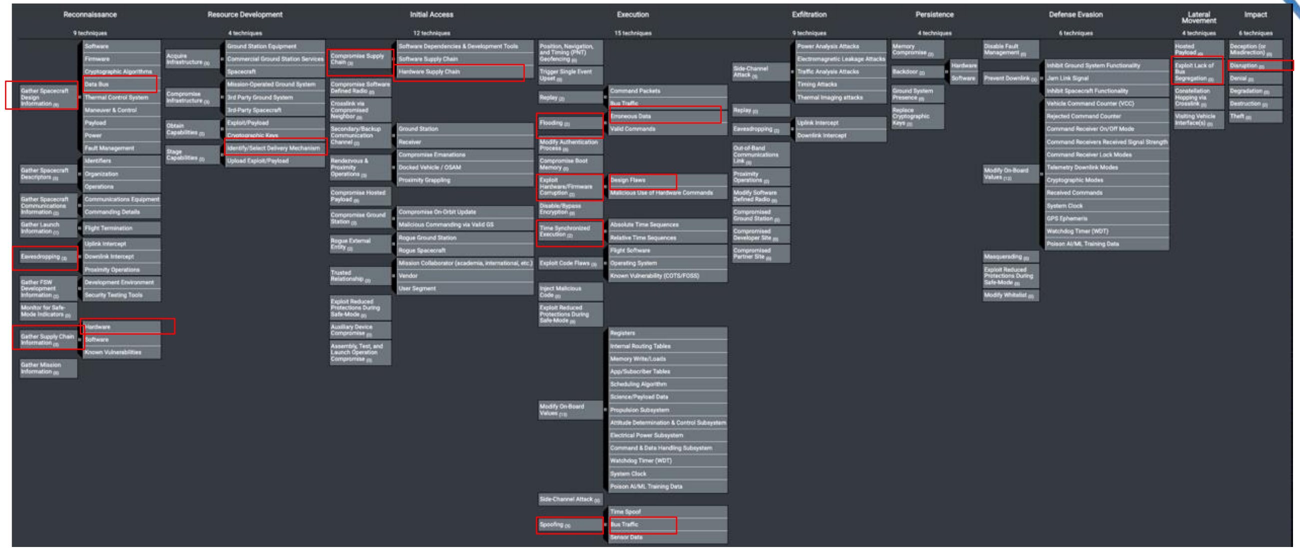


Fresh Off the Press - PCspooF

* Collaboration with Tim Dafoe, Security Researcher

https://web.eecs.umich.edu/~barisk/public/pcspoof.pdf | https://www.youtube.com/watch?v=tw1QLVQw8Go | https://aerospacecorp.medium.com/sparta-cyber-security-for-space-missions-4876f789e41c

*
- Reconnaissance [ST0001]
  - Gather Spacecraft Design Information [REC-0001]
    - Data Bus [REC-0001.04] (i.e., gather any information required for successful EMI attack and PCF spoofing — e.g., a likely virtual link ID)
  - Gather Supply Chain Information [REC-0008]
    - Hardware [REC-0008.01] (i.e., gather any information on the hardware in use, TTE utilization, EMI target, etc.)
  - Eavesdropping [REC-0005] (i.e., eavesdropping on the network, listening to device responses to learn enough to spoof PCFs)
- Resource Development [ST0002]
  - Stage Capabilities [RD-0004]
    - Identify/Select Delivery Mechanism [RD-0004.01] (i.e., identify the ideal BE device or other hardware to target and implant)
- Initial Access [ST0003]
  - Compromise Supply Chain [IA-0001]
    - Hardware Supply Chain [IA-0001.03] (i.e., conduct the activity to place a potential best-effort traffic [BE] device or other hardware implant)
  - Auxiliary Device Compromise [IA-0011] (i.e., potential for use of a generic/USB hardware vector)
- Execution [ST0004]
  - Time Synchronized Execution [EX-0008]
  - Flooding [EX-0013]
    - Erroneous Data [EX-0013.02] (i.e., generate forged ARP and the malicious EMI to target TTE switch hardware)
  - Exploit Hardware/Firmware Corruption [EX-0005]
    - Design Flaws [EX-0005.01] (i.e., exploit the weaknesses that allow for forged ARP polling of BE devices, collecting information, and spoofing of PCFs — e.g., ability to infer/determine/brute-force virtual link ID and critical traffic marker, long preamble abuse)
  - Spoofing [EX-0014]
    - Bus Traffic [EX-0014.02] (i.e., conduct the actual exploitation via injection of spoofed PCFs)
- Lateral Movement [ST0007]
  - Exploit Lack of Bus Segregation [LM-0002] (i.e., due to critical/non-critical components sharing the same physical networking infrastructure, this attack enables non-critical hardware components to affect critical components)
- Impact [ST0010]
  - Disruption [IMP-0003] (i.e., sync broken, critical actions not being performed, disruption to critical SV operations/manoeuvring, risk to mission)



The latest vulnerability disclosure and attack chain analysis shows immediate value – days after disclosure

PCspooF Countermeasure Samples

Quick Way to Identify Potential Mitigations

Segmentation

Identify the key system components or capabilities that require isolation through physical or logical means. Information should not be allowed to flow between partitioned applications unless explicitly permitted by security policy. Isolate mission critical functionality from non-mission critical functionality by means of an isolation boundary (implemented via partitions) that controls access to and protects the integrity of, the hardware, software, and firmware that provides that functionality. Enforce approved authorizations for controlling the flow of information within the spacecraft and between interconnected systems based on the defined security policy that information does not leave the spacecraft boundary unless it is encrypted. Implement boundary protections to separate bus, communications, and payload components supporting their respective functions.

ID: CM0038
Created: 2022/10/19
Last Modified: 2022/10/19

Sources

- https://attack.mitre.org/mitigations/M1030/

- -16(3) - Transmission of Security and Privacy Attributes | Cryptographic Binding
- -2(2) - Separation of System and User Functionality | Disassociability
- -3 - Security Function Isolation
- -32(1) - System Partitioning | Separate Physical Domains for Privileged Functions
- -39 - Process Isolation
- -4 - Information in Shared System Resources
- -49 - Hardware-enforced Separation and Policy Enforcement
- -50 - Software-enforced Separation and Policy Enforcement
- -6 - Resource Availability
- -7(21) - Boundary Protection | Isolation of System Components
- -7(29) - Boundary Protection | Separate Subnets to Isolate Functions

Original Component Manufacturer

Components that cannot be procured from the original component manufacturer or their authorized franchised distribution network should be approved by the supply cha… prevent and detect counterfeit and fraudulent parts and materials.

Best Segment for Countermeasure Deployment

- Development Environment

Informational References

- AC-20(5) - Use of External Systems | Portable Storage Devices — Prohibit…
- PM-30 - Supply Chain Risk Management Strategy
- PM-30(1) - Supply Chain Risk Management Strategy | Suppliers of Critica… essential Items
- RA-3(1) - Risk Assessment | Supply Chain Risk Assessment
- SR-1 - Policy and Procedures
- SR-11 - Component Authenticity
- SR-2 - Supply Chain…
- SR-2(1) - Supply Ch…
- SR-3 - Supply Chain…
- SR-3(1) - Supply Ch…

Techniques

ID	Name
IA-0001	Comprom… Chain
.03	Hardware… Chain
IA-0002	Comprom…

Dynamic Analysis

Employ dynamic analysis (e.g., using simulation, penetration te… commercial, or third-party developed code). Testing should occ… procedures (TTPs), and tools; and (3) throughout the lifecycle…

Best Segment for Countermeas…

- Ground Segment and Development Environment

Informational References

- CA-8 - Penetration Testing
- CP-4(5) - Contingency Plan Testing | Self-challenge
- RA-5(11) - Vulnerability Monitoring and Scanning | Public…
- SA-11(5) - Developer Testing and Evaluation | Penetration…
- SA-11(8) - Developer Testing and Evaluation | Dynamic C…
- SA-11(9) - Developer Testing and Evaluation | Interactive…
- SC-2(2) - Separation of System and User Functionality | D…
- SC-7(29) - Boundary Protection | Separate Subnets to Isol…
- SR-6(1) - Supplier Assessments and Reviews | Testing an…

Techniques Addressed by Cour…

ID	Name	Description
IA-0001	Compromise Supply Chain	Threat actors may ma…
.02	Software Supply Chain	Threat actors may ma… manipulation of the u…
.03	Hardware Supply Chain	Threat actors may ma… when they modify the…
IA-0007	Compromise Ground Station	Threat actors may initially compromise the ground station in order to access the target SV. Once compromised, the threat actor can perform a multitude of initial access techniques, including replay, comp… encryption keys, and compromising authentication schemes.
.01	Compromise On Orbit…	Threat actors may manipulate and modify on-orbit updates before they are sent to the target SV. This attack can be done in a number of ways, including manipulation of source code, manipulating environ…

On-board Intrusion Detection & Prevention

Utilize on-board intrusion detection/prevention system that monitors the mission critical components or systems and audit/logs actions. The IDS/IPS should have the capability to respond to threats and it should address signature-based attacks along with dynamic never-before seen attacks using machine learning/adaptive technologies. The IDS/IPS must integrate with traditional fault management to provide a wholistic approach to faults on-board the spacecraft. Spacecraft should select and execute safe countermeasures against cyber-attacks. These countermeasures are a ready supply of options to triage against the specific types of attack and mission priorities. Minimally, the response should ensure vehicle safety and continued operations. Ideally, the goal is to trap the threat, convince the threat that it is successful, and trace and track the attacker — with or without ground support. This would support successful attribution and evolving countermeasures to mitigate the threat in the future. "Safe countermeasures" are those that are compatible with the system's fault management system to avoid unintended effects or fratricide on the system.

ID: CM0032
Created: 2022/1…
Last Modified: 2…

Sources

- https://attack.mitre.org/mitigations/M1031/

Best Segment for Countermeasure Deployment

- Space Segment

Informational References

- AU-14 - Session Audit
- AU-2 - Event Logging
- AU-3 - Content of Audit Records
- AU-3(1) - Content of Audit Records | Additional Audit Information
- AU-4 - Audit Log Storage Capacity
- AU-4(1) - Audit Log Storage Capacity | Transfer to Alternate Storage
- AU-5 - Response to Audit Logging Process Failures
- AU-5(2) - Response to Audit Logging Process Failures | Real-time Alerts
- AU-5(5) - Response to Audit Logging Process Failures | Alternate Audit Logging Capability
- AU-6(1) - Audit Record Review, Analysis, and Reporting | Automated Process Integration
- AU-6(4) - Audit Record Review, Analysis, and Reporting | Central Review and Analysis
- AU-8 - Time Stamps
- AU-9 - Protection of Audit Information
- AU-9(2) - Protection of Audit Information | Store on Separate Physical Systems or Components
- AU-9(3) - Protection of Audit Information | Cryptographic Protection
- CA-7(6) - Continuous Monitoring | Automation Support for Monitoring
- CM-11(3) - User-installed Software | Automated Enforcement and Monitoring
- CP-10 - System Recovery and Reconstitution
- CP-10(4) - System Recovery and Reconstitution | Restore Within Time Period
- IR-4 - Incident Handling
- IR-4(11) - Incident Handling | Integrated Incident Response Team
- IR-4(12) - Incident Handling | Malicious Code and Forensic Analysis
- IR-4(14) - Incident Handling | Security Operations Center
- IR-5 - Incident Monitoring

Techniques Addressed by Countermeasure

Authentication

Authenticate all communication sessions (crosslink and ground stations) for all commands before establishing remote connections using bidirectional authentication that is cryptographically based. Adding authentication on the spacecraft bus and communications on-board the spacecraft is also recommended.

ID: CM0031
Created: 2022/10/19
Last Modified: 2022/10/19

Best Segment for Countermeasure Deployment

- Space Segment

Informational References

- AC-17(10) - Remote Access | Authenticate Remote Commands
- AC-17(2) - Remote Access | Protection of Confidentiality and Integrity Using Encryption
- AC-18(1) - Wireless Access | Authentication and Encryption
- IA-3(1) - Device Identification and Authentication | Cryptographic Bidirectional Authentication
- IA-4 - Identifier Management
- IA-4(9) - Identifier Management | Attribute Maintenance and Protection
- IA-7 - Cryptographic Module Authentication
- SA-8(15) - Security and Privacy Engineering Principles | Predicate Permission
- SA-8(9) - Security and Privacy Engineering Principles | Trusted Components
- SC-16(2) - Transmission of Security and Privacy Attributes | Anti-spoofing Mechanisms
- SC-32(1) - System Partitioning | Separate Physical Domains for Privileged Functions
- SC-7(11) - Boundary Protection | Restrict Incoming Communications Traffic
- SI-14(3) - Non-persistent | Non-persistent Connectivity

Techniques Addressed by Countermeasure

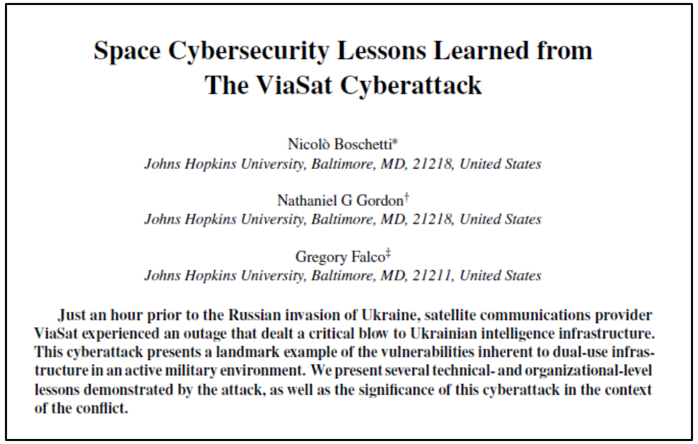
ID	Name	Description
IA-0003	Crosslink via Compromised Neighbor	Threat actors may compromise a victim SV via the crosslink communications of a neighboring SV that has been compromised. SVs in close proximity are able to send commands back and forth. Threat ac… compromise other SVs once they have access to another that is nearby.
EX-0001	Replay	Replay attacks involve threat actors recording previously data streams and then resending them at a later time. This attack can be used to fingerprint systems, gain elevated privileges, or even cause a den…
.01	Command Packets	Threat actors may interact with the victim SV by replaying captured commands to the SV. While not necessarily malicious in nature, replayed commands can be used to overload the target SV and cause it'… attack, or monitor various responses by the SV. If critical commands are captured and replayed, thruster fires, then the impact could impact the SV's attitude control/orbit.
EX-0006	Disable/Bypass…	Threat actors may perform specific techniques in order to bypass or disable the encryption mechanism onboard the victim SV. By bypassing or disabling this particular mechanism, further tactics can be p…

…within visual contact or close…
…e to deploy malware to latera…
…has the ability to connect via…
…pecific command set. The co… …y to command hosted payloa…

Use Case Example

Assessments / Table-Tops

Assessments / Table-Tops



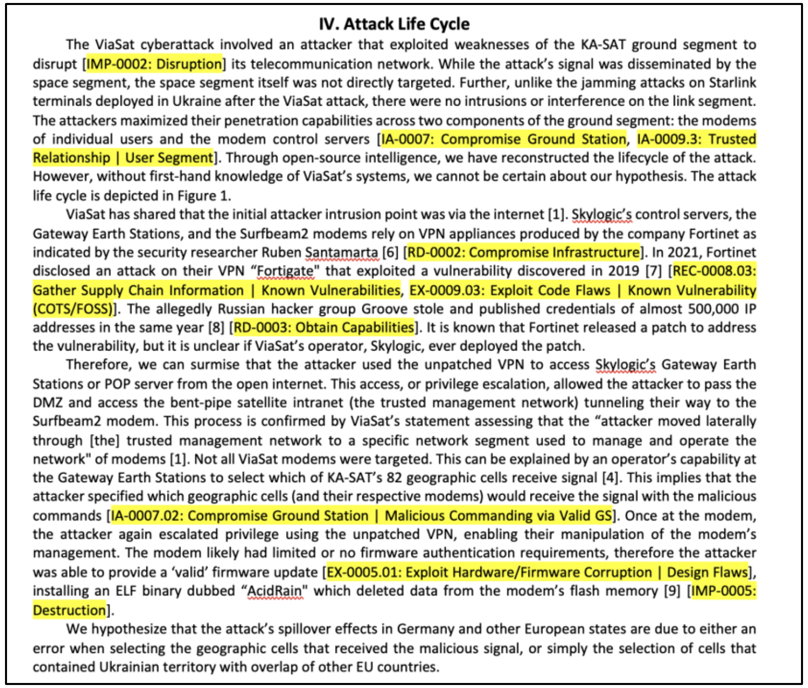
Space Cybersecurity Lessons Learned from The ViaSat Cyberattack

Nicolò Boschetti*
Johns Hopkins University, Baltimore, MD, 21218, United States

Nathaniel G Gordon†
Johns Hopkins University, Baltimore, MD, 21218, United States

Gregory Falco‡
Johns Hopkins University, Baltimore, MD, 21211, United States

Just an hour prior to the Russian invasion of Ukraine, satellite communications provider ViaSat experienced an outage that dealt a critical blow to Ukrainian intelligence infrastructure. This cyberattack presents a landmark example of the vulnerabilities inherent to dual-use infrastructure in an active military environment. We present several technical- and organizational-level lessons demonstrated by the attack, as well as the significance of this cyberattack in the context of the conflict.



IV. Attack Life Cycle

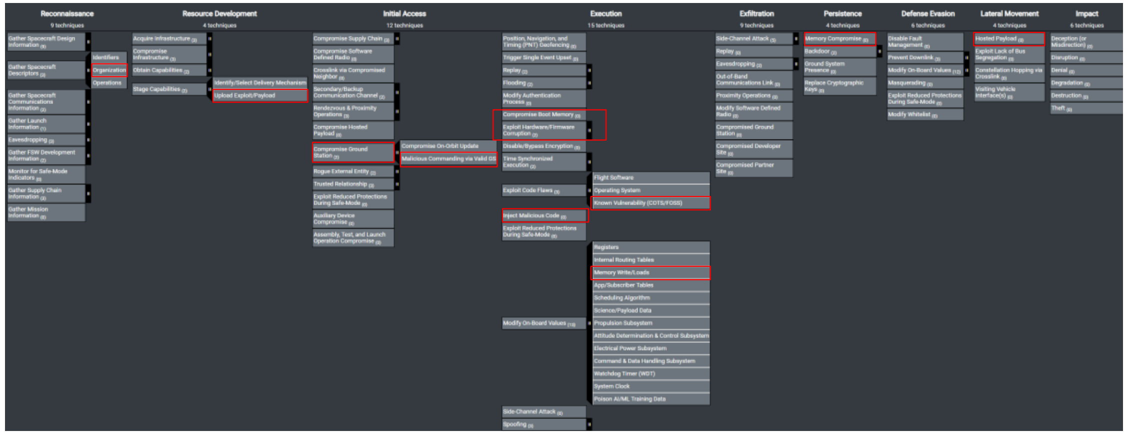
The ViaSat cyberattack involved an attacker that exploited weaknesses of the KA-SAT ground segment to disrupt [IMP-0002: Disruption] its telecommunication network. While the attack's signal was disseminated by the space segment, the space segment itself was not directly targeted. Further, unlike the jamming attacks on Starlink terminals deployed in Ukraine after the ViaSat attack, there were no intrusions or interference on the link segment. The attackers maximized their penetration capabilities across two components of the ground segment: the modems of individual users and the modem control servers [IA-0007: Compromise Ground Station, IA-0009.3: Trusted Relationship | User Segment]. Through open-source intelligence, we have reconstructed the lifecycle of the attack. However, without first-hand knowledge of ViaSat's systems, we cannot be certain about our hypothesis. The attack life cycle is depicted in Figure 1.

ViaSat has shared that the initial attacker intrusion point was via the internet [1]. Skylogic's control servers, the Gateway Earth Stations, and the Surfbeam2 modems rely on VPN appliances produced by the company Fortinet as indicated by the security researcher Ruben Santamarta [6] [RD-0002: Compromise Infrastructure]. In 2021, Fortinet disclosed an attack on their VPN "Fortigate" that exploited a vulnerability discovered in 2019 [7] [REC-0008.03: Gather Supply Chain Information | Known Vulnerabilities, EX-0009.03: Exploit Code Flaws | Known Vulnerability (COTS/FOSS)]. The allegedly Russian hacker group Groove stole and published credentials of almost 500,000 IP addresses in the same year [8] [RD-0003: Obtain Capabilities]. It is known that Fortinet released a patch to address the vulnerability, but it is unclear if ViaSat's operator, Skylogic, ever deployed the patch.

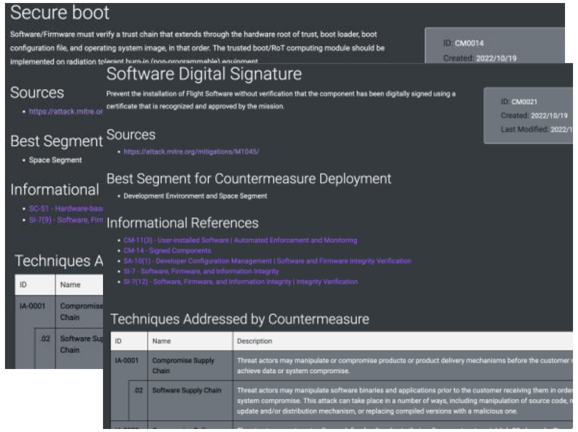
Therefore, we can surmise that the attacker used the unpatched VPN to access Skylogic's Gateway Earth Stations or POP server from the open internet. This access, or privilege escalation, allowed the attacker to pass the DMZ and access the bent-pipe satellite intranet (the trusted management network) tunneling their way to the Surfbeam2 modem. This process is confirmed by ViaSat's statement assessing that the "attacker moved laterally through [the] trusted management network to a specific network segment used to manage and operate the network" of modems [1]. Not all ViaSat modems were targeted. This can be explained by an operator's capability at the Gateway Earth Stations to select which of KA-SAT's 82 geographic cells receive signal [4]. This implies that the attacker specified which geographic cells (and their respective modems) would receive the signal with the malicious commands [IA-0007.02: Compromise Ground Station | Malicious Commanding via Valid GS]. Once at the modem, the attacker again escalated privilege using the unpatched VPN, enabling their manipulation of the modem's management. The modem likely had limited or no firmware authentication requirements, therefore the attacker was able to provide a 'valid' firmware update [EX-0005.01: Exploit Hardware/Firmware Corruption | Design Flaws], installing an ELF binary dubbed "AcidRain" which deleted data from the modem's flash memory [9] [IMP-0005: Destruction].

We hypothesize that the attack's spillover effects in Germany and other European states are due to either an error when selecting the geographic cells that received the malicious signal, or simply the selection of cells that contained Ukrainian territory with overlap of other EU countries.

APT Attack Chain Emulation for Test/Tabletop Procedure Development



Tabletop Countermeasure



<u>Like with Threat Intel Reporting, can recreate attack chain in SPARTA to tabletop countermeasures for kill chain</u>

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Assessments / Table-Tops

Authority to Operate / NIST 800-53 Assessments

- *When controls are de-scoped (i.e., AC-4) – the assessor will now have a resource to understand which TTPs and potential countermeasures are associated with the control*
  - *Provides additional context to make risk-based decision during ATO*

AC-4

Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: organization-defined information flow control policies].

Informational References

- https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-4/

Assessors and Authorizing Officials can better assess impact of control failures and understand the types of capabilities necessary on a spacecraft to meet the control's intent

Countermeasures Covered by Control

ID	Name	Description
CM0050	On-board Messag Encryption	
CM0005	Ground-based Countermeasures	
CM0038	Segmentation	identify the key system com to flow between partitioned critical functionality by mea hardware, software, and firm within the spacecraft and be spacecraft boundary unless supporting their respective f

Space Threats Tagged by Control

ID	Description
SV-AC-6	Three main parts of attack on CPU (FPG payloads are all thre fault injector for 155 from the OS or FSW

Related SPARTA Techniques and Sub-Techniques

ID	Name	Description
IA-0005	Rendezvous & Proximity Operations	Threat actors may perform a space rendezvous w orbit and approach to a very close distance (e.g. v
IA-0005.02	Docked Vehicle / OSAM	Threat actors may leverage docking vehicles to la actor may target vehicles on the ground or in spa docking interface.
IA-0005.03	Proximity Grappling	Threat actors may posses the capability to grapp proximity / rendezvous perspective a threat actor once it has grappled the target SV, they could per
IA-0006	Compromise Hosted Payload	Threat actors may compromise the target SV hos can usually be accessed from the ground via a sp infrastructure or some host payloads have their o may be able to leverage the ability to command h compromise the system. Depending on the imple
IA-0007	Compromise Ground Station	Threat actors may initially compromise the groun perform a multitude of initial access techniques, i and compromising authentication schemes.
IA-0007.01	Compromise On-Orbit Update	Threat actors may manipulate and modify on-orbi of ways, including manipulation of source code, r compiled versions with a malicious one.
IA-0007.02	Malicious Commanding via	Threat actors may compromise target owned gro software, etc.) that can be used for future campai

Requirement

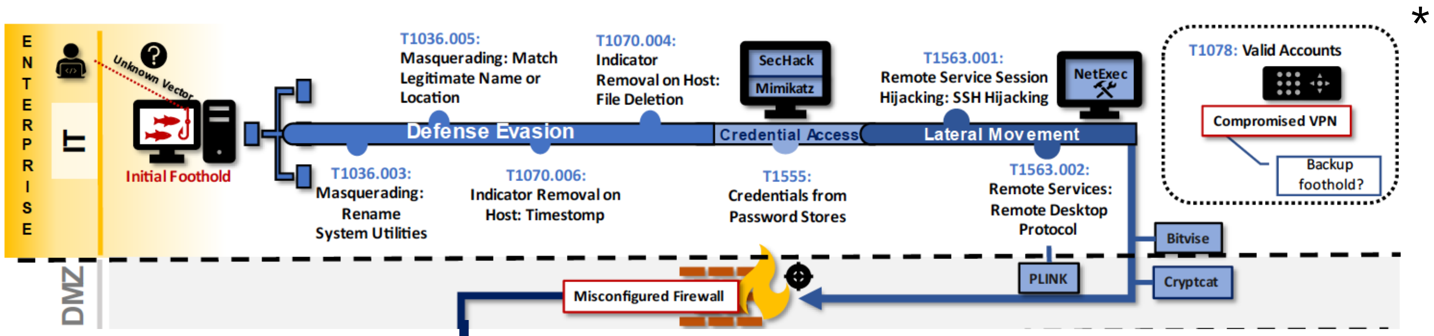
The [Program-defined security policy] shall state that information should not be allowed to flow between partitioned applications unless explicitly permitted by the Program's security policy. {SV-AC-6} {AC-4}

The spacecraft shall enforce approved authorizations for controlling the flow of information within the spacecraft and between interconnected systems based on the [Program defined security policy] that information does not leave the spacecraft boundary unless it is encrypted. {SV-AC-6} {AC-4}

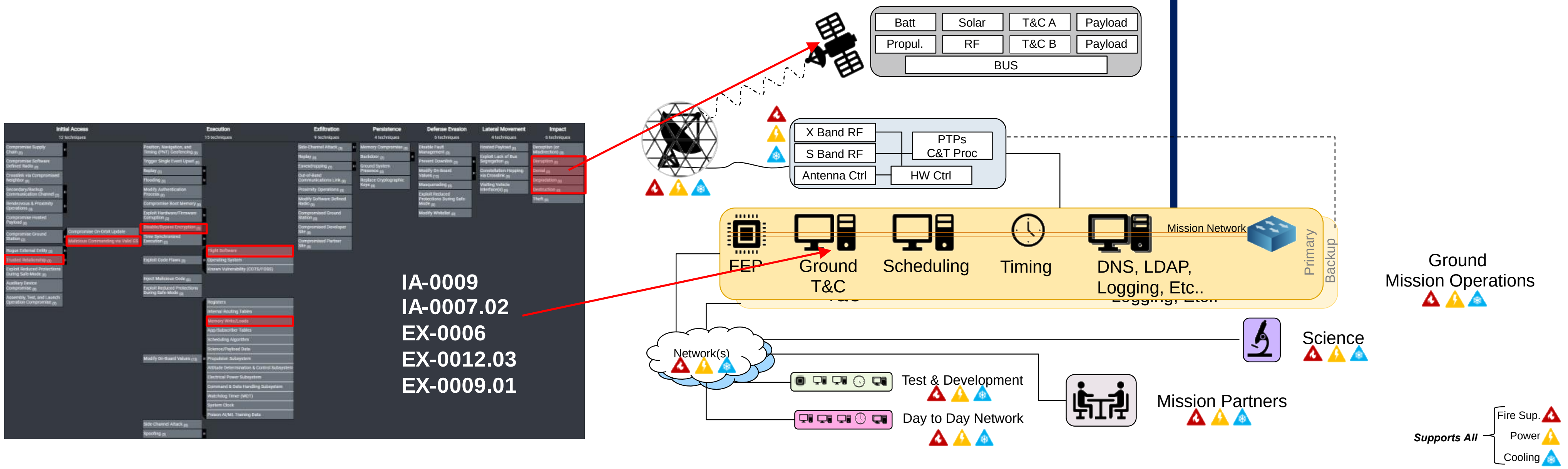
Assessments

Full End to End Analysis using TTPs

- When doing assessments on space ports, potentially leveraging SPARTA to perform analysis
- Some combination of SPARTA and MITRE ATT&CK can be used to identify attack chains and pivot points using known TTPs
- Focus can be applied on **gaps** in existing countermeasure/defenses
  - *Can provide links to countermeasures with relevant guidance to stakeholders*



*

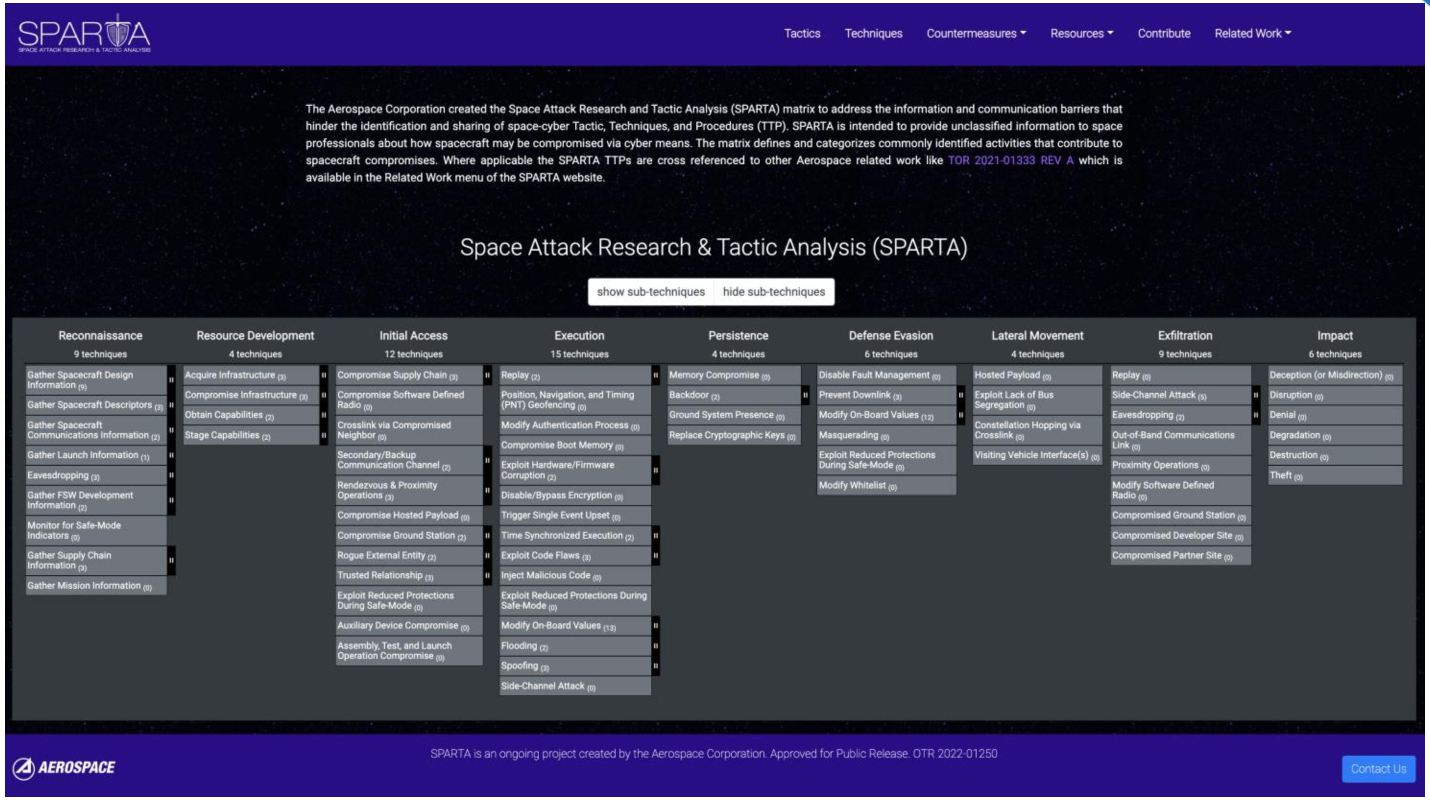


* MP220278 MITRE PRODUCT - Platform Independent Vectors of Techniques (PIVOT)

SPARTA

SPACE ATTACK RESEARCH & TACTIC ANALYSIS

https://sparta.aerospace.org



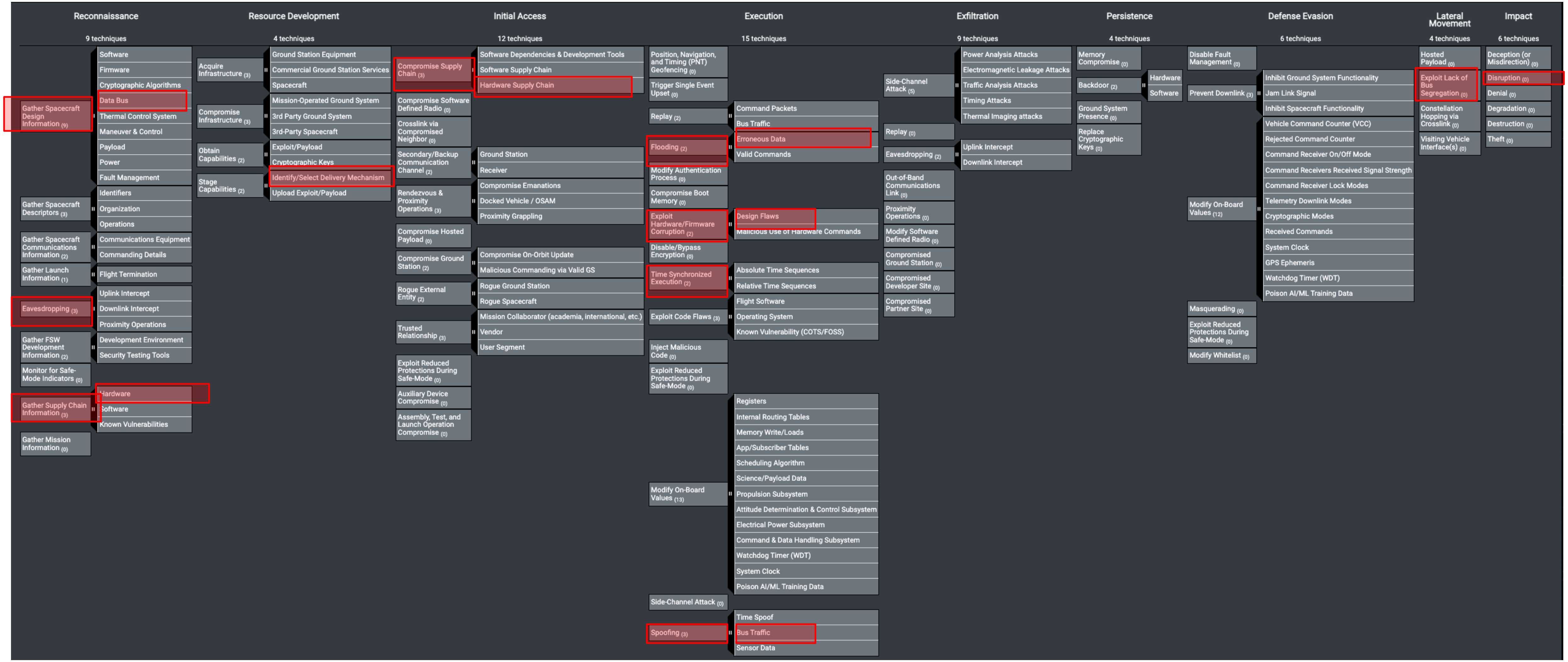
Key SPARTA Links:

- Getting Started with SPARTA: https://sparta.aerospace.org/resources/getting-started
- 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
- FAQ: https://sparta.aerospace.org/resources/faq
- Matrix: https://sparta.aerospace.org
- Related Work: https://sparta.aerospace.org/related-work/did-space with ties into TOR 2021-01333 REV A

Backup

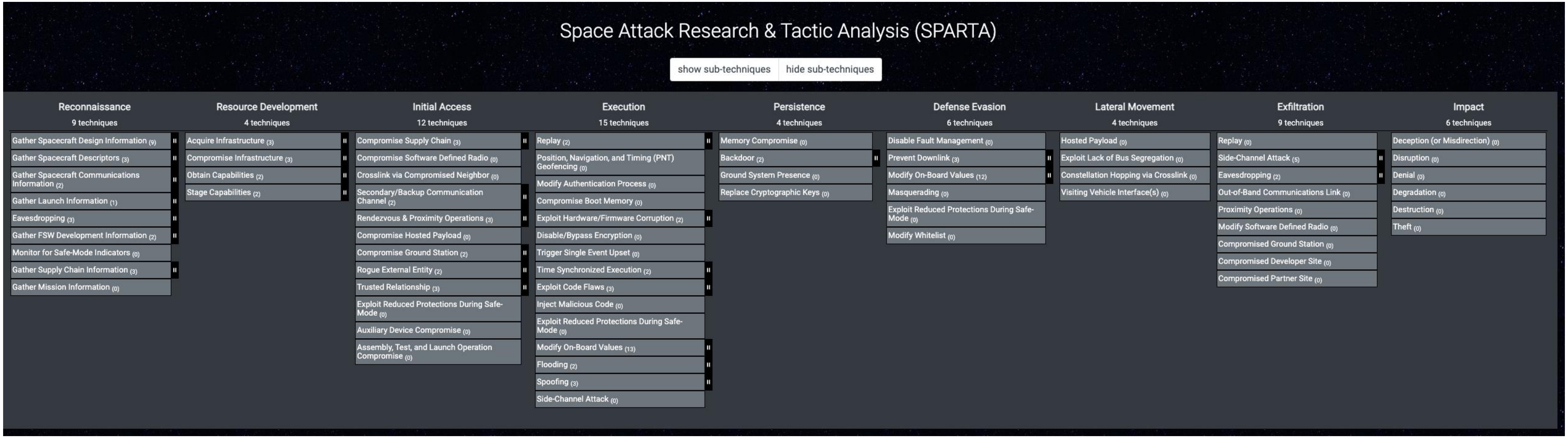
SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

PCspooF Potential Attack Chain



SPARTA Framework

Only Tactics and Techniques

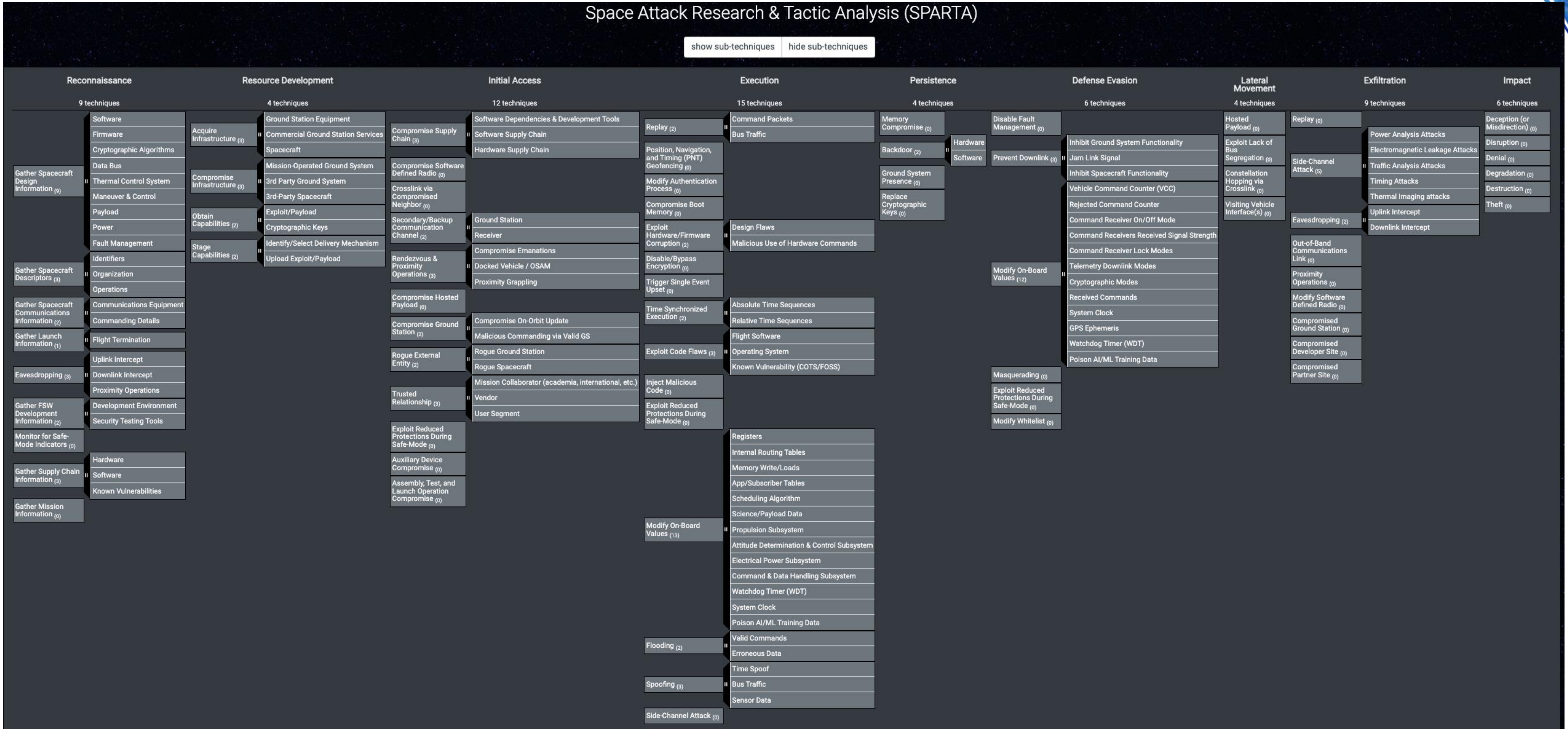


https://sparta.aerospace.org

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

SPARTA

Tactics, Techniques with Sub-Techniques Expanded



Example - Sub-Technique

Key Framework Elements

Description

Parent Technique Link

Correlation to TOR 2021-01333 Threat IDs and resources

If any loose correlation to known TTPs from MITRE ATT&CK.

Helps tie in existing/historical intel reports

Potential Countermeasures

NIST Rev 5 Correlation

Rogue Ground Station

Threat actors may gain access to a victim SV through the use of a rogue ground system. With this technique, the threat actor does not need access to a legitimate ground station or communication site.

ID: IA-0008.01

Sub-technique of: IA-0008

Related Aerospace Threat IDs: SV-AC-1 | SV-AC-2 | SV-IT-1 | SV-CF-2

Related MITRE ATT&CK TTPs: T1133

Tactic: Initial Access

Created: 2022/08/22

Last Modified: 2022/10/03

Countermeasures

ID	Name	Description	NIST Rev5
CM0002	COMSEC	Utilizing secure communication protocols with strong cryptographic mechanisms to prevent unauthorized disclosure of, and detect changes to, information during transmission. Systems should also maintain the confidentiality and integrity of information during preparation for transmission and during reception. Spacecraft should not employ a mode of operations where cryptography on the TT&C link can be disabled (i.e., crypto-bypass mode). The cryptographic mechanisms should identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.	IA-5(7) | SI-10(3) | AC-2(11) | AC-3(10) | IA-5 | IA-7 | SC-10 | SC-12 | SC-12(1) | SC-12(2) | SC-12(3) | SC-13 | SC-28(1) | SC-7 | SC-7(11) | SC-7(18) | AC-17(10) | SI-10 | SI-10(5) | AC-17(1) | AC-17(2) | AC-18(1)
CM0030	Crypto Key Management	Leverage best practices for crypto key management as defined by organization like NIST or the National Security Agency. Leverage only approved cryptographic algorithms, cryptographic key generation algorithms or key distribution techniques, authentication techniques, or evaluation criteria. Encryption key handling should be performed outside of the onboard software and protected using cryptography. Encryption keys should be restricted so that they cannot be read via any telecommands.	SC-12 | SC-12(1) | SC-12(2) | SC-12(3)
CM0033	Relay Protection	Implement relay and replay-resistant authentication mechanisms for establishing a remote connection or connections on the spacecraft bus.	IA-2(8) | IA-3 | IA-3(1) | IA-4 | IA-7 | SC-13 | SC-23 | SC-7 | SC-7(11) | SC-7(18) | AC-17(10) | SI-10 | SI-10(5)
CM0055	Secure Command Mode(s)	Provide additional protection modes for commanding the spacecraft. These can be where the spacecraft will restrict command lock based on geographic location of ground stations, special operational modes within the flight software, or even temporal controls where the spacecraft will only accept commands during certain times.	AC-2(11) | AC-2(12) | SC-7 | AC-3 | AC-3(2) | AC-3(3) | AC-3(4) | AC-3(8) | AC-17(1)
CM0034	Monitor Critical Telemetry Points	Monitor defined telemetry points for malicious activities (i.e., jamming attempts, commanding attempts (e.g., command modes, counters, etc.)). This would include valid/processed commands as well as commands that were rejected. Telemetry monitoring should synchronize with ground-based Defensive Cyber Operations (i.e., SIEM/auditing) to create a full space system situation awareness from a cybersecurity perspective.	SC-7 | AU-3(1) | AC-17(1)
CM0032	On-board Intrusion Detection & Prevention	Utilize on-board intrusion detection/prevention system that monitors the mission critical components or systems and audit/logs actions. The IDS/IPS should have the capability to respond to threats and it should address signature-based attacks along with dynamic never-before seen attacks using machine learning/adaptive technologies. The IDS/IPS must integrate with traditional fault management to provide a wholistic approach to faults on-board the spacecraft. Spacecraft should select and execute safe countermeasures against cyber-attacks. These countermeasures are a ready supply of options to triage against the specific types of attack and mission priorities. Minimally, the response should ensure vehicle safety and continued operations. Ideally, the goal is to trap the threat, convince the threat that it is successful, and trace and track the attacker — with or without ground support. This would support successful attribution and evolving countermeasures to mitigate the threat in the future. "Safe countermeasures" are those that are compatible with the system's fault management system to avoid unintended effects or fratricide on the system.	CP-10 | CP-10(4) | AU-2 | AU-3 | AU-3(1) | AU-4 | AU-4(1) | AU-5 | AU-5(2) | AU-6(1) | AU-6(4) | AU-8 | AU-9 | AU-9(2) | AU-9(3) | AU-14 | SI-4 | SI-4(2) | SI-4(4) | SI-4(10) | SI-4(16) | SI-4(5) | SI-6 | SI-7(8) | SI-16 | IR-4 | IR-5 | IR-5(1) | SC-5(3) | SC-7(9) | SI-17 | SI-4(11)

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Countermeasures

SPARTA Countermeasures

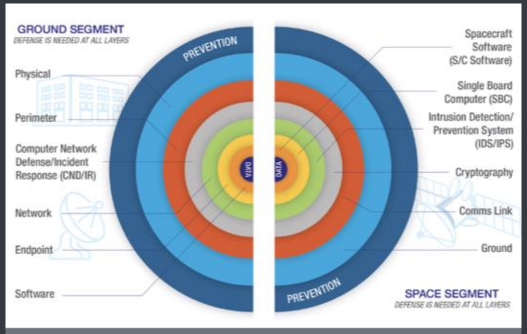
Countermeasures represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed. The below table view not only describes the countermeasure, it also provides informative references to the NIST Risk Management Framework (RMF) revision 5 control identifier. Each NIST control ID is a hyperlink to more information on the control itself. This mapping is meant to be informative and provide traceability to common standards that are being leveraged within the space community. In addition to the table view, there is a Defense-in-Depth (DiD) view that provides the countermeasures overlaid onto Aerospace's DiD model for space systems which was discussed in TOR 2021-01333 REV A. When selecting a specific countermeasure the following information will be displayed: description of the countermeasure, the best segment for countermeasure deployment, any informative references as well as any techniques that the countermeasure addresses. The mapping to countermeasure to technique(s) are a one to many relationship. For the best segment for countermeasure deployment, this is meant to articulate the ideal place to deploy the countermeasure leveraging the following choices: space segment, the development environment, or the ground segment. The space segment is considered to be the spacecraft or spacecrafts if within a constellation. The development segment captures the factories, hardware foundries, the software development organization as well as the Assembly, Test and Launch Operations (ATLO) facilities. The ground segment is meant to capture the operational and maintenance areas for the ground system. This includes the mission operations environments, the antenna environments, the back haul networks, as well as any management network segments for vendors or commercial entities.

Table View | DiD View

ID	Name	Description	NIST Rev5 Controls
CM0000	Countermeasure Not Identified	This technique is a result of utilizing TTPs to create an impact and the applicable countermeasures are associated with the TTPs leveraged to achieve the impact	None
CM0001	Protect Sensitive Information	Organizations should look to identify and properly classify mission sensitive design/operations information (e.g., fault management approach) and apply access control accordingly. Any location (ground system, contractor networks, etc.) storing design information needs to ensure design info is protected from exposure, exfiltration, etc. Space system sensitive information may be classified as Controlled Unclassified Information (CUI) or Company Proprietary. Space system sensitive information can typically include a wide range of candidate material: the functional and performance specifications, any ICDs (like radio frequency, ground-to-space, etc.), command and telemetry databases, scripts, simulation and rehearsal results/reports, descriptions of uplink protection including any disabling/bypass features, failure/anomaly resolution, and any other sensitive information related to architecture, software, and flight/ground /mission operations. This could all need protection at the appropriate level (e.g., unclassified, CUI, proprietary, classified, etc.) to mitigate levels of cyber intrusions that may be conducted against the project's networks. Stand-alone systems and/or separate database encryption may be needed with controlled access and on-going Configuration Management to ensure changes in command procedures and critical database areas are tracked, controlled, and fully tested to avoid loss of science or the entire mission. Sensitive documentation should only be accessed by personnel with defined roles and a need to know. Well established access controls (roles, encryption at rest and transit, etc.) and data loss prevention (DLP) technology are key countermeasures. The DLP should be configured for the specific data types in question.	AC-3(11) | AC-4(23) | AC-4(25) | CM-12 | CM-12(1) | PM-11 | PM-17 | SA-3(1) | SA-3(2) | SA-4(12) | SA-5 | SA-9(7) | SI-21 | SI-23 | SR-12 | SR-7
CM0008	Security Testing Results	As penetration testing and vulnerability scanning is a best practice, protecting the results from these tests and scans is equally important. These reports and results typically outline detailed vulnerabilities and how to exploit them. As with countermeasure CM0001, protecting sensitive information from disclosure to threat actors is imperative.	AC-3(11) | CA-8 | RA-5 | RA-5(11) | SA-11(5) | SA-5
CM0009	Threat Intelligence Program	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities and mitigate risk. Leverage all-source intelligence services or commercial satellite imagery to identify and track adversary infrastructure development/acquisition. Countermeasures for this attack fall outside the scope of the mission in the majority of cases.	PM-16 | PM-16(1) | PM16(1) | RA-10 | RA-3(2) | RA-3(3) | SR-8
CM0020	Threat modeling	Use threat modeling and vulnerability analysis to inform the current development process using analysis from similar systems, components, or services where applicable.	SA-11(2) | SA-15(8)
CM0022	Criticality Analysis	Conduct a criticality analysis to identify mission critical functions, critical components, and data flows and reduce the vulnerability of such functions and components through secure system design. Focus supply chain protection on the most critical components/functions. Leverage other countermeasures like segmentation and least privilege to protect the critical components.	CP-2(8) | PM-11 | PM-17 | PM-30 | PM-30(1) | PM-32 | RA-3(1) | RA-9 | RA-9 | SA-15(3) | SC-32(1) | SC-7(29) | SR-1 | SR-1 | SR-2 | SR-2(1) | SR-3 | SR-3(2) | SR-3(3) | SR-5(1) | SR-7

Table View | DiD View

Data	Spacecraft Software	Single Board Computer	IDS/IPS	Cryptography	Comms Link	Ground	Prevention
TEMPEST	Development Environment Security	Secure boot	Cloaking Safe-mode	COMSEC	TRANSEC	Ground-based Countermeasures	Protect Sensitive Information
Shared Resource Leakage	Software Version Numbers	Disable Physical Ports	On-board Intrusion Detection & Prevention	Crypto Key Management		Monitor Critical Telemetry Points	Security Testing Results
Machine Learning Data Integrity	Update Software	Segmentation	Robust Fault Management	Authentication		Protect Authenticators	Threat Intelligence Program
On-board Message Encryption	Vulnerability Scanning	Backdoor Commands	Cyber-safe Mode	Relay Protection		Physical Security Controls	Threat modeling
	Software Bill of Materials	Error Detection and Correcting Memory	Fault Injection Redundancy			Data Backup	Criticality Analysis
	Dependency Confusion	Resilient On-board Timing	Model-based System Verification			Alternate Communications Paths	Anti-counterfeit Hardware
	Software Source Control	Tamper Resistant Body	Smart Contracts				Supplier Review
	CWE List	Power Randomization	Reinforcement Learning				Original Component Manufacturer
	Coding Standard	Power Consumption Obfuscation					ASIC/FPGA Manufacturing
	Dynamic Analysis	Secret Shares					Tamper Protection
	Static Analysis	Power Masking					User Training
	Software Digital Signature	Increase Clock Cycles/Timing					Insider Threat Protection
	Configuration Management	Dual Layer Protection					Two-Person Rule
	Session Termination	OSAM Dual Authorization					
	Least Privilege						
	Long Duration Testing						
	Operating System Security						
	Secure Command Mode(s)						
	Dummy Process - Aggregator Node						
	Process White Listing						



Countermeasures

Cross Referencing / Organizing Information

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Techniques | Countermeasures | Resources | Contribute | Related Work

COUNTERMEASURES

SPARTA by DiD Layer
- Data
- Spacecraft Software
- Single Board Computer
- IDS/IPS
- Cryptography
- Comms Link
- Ground
- Prevention

Software Bill of Materials

Generate Software Bill of Materials (SBOM) against the entire software supply chain and cross correlate with known vulnerabilities (e.g., Common Vulnerabilities and Exposures) to mitigate known vulnerabilities. Protect the SBOM according to countermeasures in CM0001.

ID: CM0012
Created: 2022/09/27
Last Modified: 2022/09/27

Best Segment for Countermeasure Deployment

- Development Environment

Informational References

- CM-10(1) - Software Usage Restrictions | Open-source Software
- CM-8 - System Component Inventory
- CM-8(7) - System Component Inventory | Centralized Repository

Techniques Addressed by Countermeasure

ID		Name	Description
IA-0001		Compromise Supply Chain	Threat actors may manipulate or compromise products or product delivery mechanisms before the customer receives them in order to achieve data or system compromise.
	.01	Software Dependencies & Development Tools	Threat actors may manipulate software dependencies (i.e. dependency confusion) and/or development tools prior to the customer receiving them in order to achieve data or system compromise. Software binaries and applications often depend on external software to function properly. spacecraft developers may use open source projects to help with their creation. These open source projects may be targeted by threat actors as a way to add malicious code to the victim spacecraft's dependencies.
	.02	Software Supply Chain	Threat actors may manipulate software binaries and applications prior to the customer receiving them in order to achieve data or system compromise. This attack can take place in a number of ways, including manipulation of source code, manipulation of the update and/or distribution mechanism, or replacing compiled versions with a malicious one.
IA-0002		Compromise Software Defined Radio	Threat actors may target software defined radios due to their software nature to establish command and control channels. Since SDRs are programmable, when combined with supply chain or development environment attacks, SDRs provide a pathway to setup covert command and control channels for a threat actor.
IA-0007		Compromise Ground Station	Threat actors may initially compromise the ground station in order to access the target spacecraft. Once compromised, the threat actor can perform a multitude of initial access techniques, including replay, compromising flight software deployment, compromising encryption keys, and compromising authentication schemes.
	.01	Compromise On-Orbit Update	Threat actors may manipulate and modify on-orbit updates before they are sent to the target spacecraft. This attack can be done in a number of ways, including manipulation of source code, manipulating environment variables, on-board table/memory values, or replacing compiled versions with a malicious one.
EX-0009		Exploit Code Flaws	Threats actors may identify and exploit flaws or weaknesses within the software running on-board the target spacecraft. These attacks may be extremely targeted and tailored to specific coding errors introduced as a result of poor coding practices or they may target known issues in the commercial software components.
	.01	Flight Software	Threat actors may abuse known or unknown flight software code flaws in order to further the attack campaign. In some cases, these code flaws can perpetuate throughout the victim spacecraft, allowing access to otherwise segmented subsystems.
	.02	Operating System	Threat actors may exploit flaws in the operating system code, which controls the storage, memory management, provides resources to the flight software, and controls the bus.
	.03	Known Vulnerability (COTS/FOSS)	Threat actors may utilize knowledge of the spacecraft software composition to enumerate and exploit known flaws or vulnerabilities in the commercial or open source software running on-board the target spacecraft.

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

NIST Correlations

SC-7(11)

Only allow incoming communications from [Assignment: organization-defined authorized sources] to be routed to [Assignment: organization-defined authorized destinations].

ID: SC-7(11)
Enhancement of : SC-7
Created: 2022/10/19
Last Modified: 2022/10/19

Informational References

- https://csf.tools/reference/nist-sp-800-53/r5/sc/sc-7/sc-7-11/

Countermeasures Covered by Control

ID	Name	Description
CM0002	COMSEC	Utilizing secure communication protocols with strong cryptographic mechanisms to prevent unauthorized disclosure of, and detect changes to, information during transmission. Systems should also maintain the confidentiality and integrity of information during preparation for transmission and during reception. Spacecraft should not employ a mode of operations where cryptography on the TT&C link can be disabled (i.e., crypto-bypass mode). The cryptographic mechanisms should identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.
CM0031	Authentication	Authenticate all communication sessions (crosslink and ground stations) for all commands before establishing remote connections using bidirectional authentication that is cryptographically based. Adding authentication on the spacecraft bus and communications on-board the spacecraft is also recommended.
CM0033	Relay Protection	Implement relay and replay-resistant authentication mechanisms for establishing a remote connection or connections on the spacecraft bus.
CM0005	Ground-based Countermeasures	This countermeasure is focused on the protection of terrestrial assets like ground networks and development environments/contractor networks, etc. Traditional detection technologies and capabilities would be applicable here. Utilizing resources from NIST CSF to properly secure these environments using identify, protect, detect, recover, and respond is likely warranted. Additionally, NISTIR 8401 may provide resources as well since it was developed to focus on ground-based security for space systems (https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.pdf). Furthermore, the MITRE ATT&CK framework provides IT focused TTPs and their mitigations https://attack.mitre.org/mitigations/enterprise/. Several recommended NIST 800-53 Rev5 controls are provided for reference when designing ground systems/networks.

Space Threats Tagged by Control

ID	Description
SV-AC-1	Attempting access to an access-controlled system resulting in unauthorized access
SV-AC-2	Replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction

Related SPARTA Techniques and Sub-Techniques

ID	Name	Description
REC-0001	Gather Spacecraft Design Information	Threat actors may gather information about the victim SV's design that can be used for future campaigns or to help perpetuate other techniques. Information about the SV can include software, firmware, encryption type, purpose, as well as various makes and models of subsystems.
REC-0001.01	Software	Threat actors may gather information about the victim SV's internal software that can be used for future campaigns or to help perpetuate other techniques. Information (e.g. source code, binaries, etc.) about commercial, open-source, or custom developed software may include a variety of details such as types, versions, and memory maps. Leveraging this information threat actors may target vendors of operating systems, flight software, or open-source communities to embed backdoors or for performing reverse engineering research to support offensive cyber operations.
REC-0001.02	Firmware	Threat actors may gather information about the victim SV's firmware that can be used for future campaigns or to help perpetuate other techniques. Information about the firmware may include a variety of details such as type and versions on specific devices, which may be used to infer more information (ex. configuration, purpose, age/patch level, etc.). Leveraging this information threat actors may target firmware vendors to embed backdoors or for performing reverse engineering research to support offensive cyber operations.
REC-	Cryptographic	Threat actors may gather information about any cryptographic algorithms used on the victim SV's that can be used for future campaigns or to help perpetuate other techniques. Information about the algorithms can include type and private

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Correlated to Past Aerospace Publication(s)

SPARTA relationship to broader NIST frameworks and previous Aerospace publications

Sample requirements for engineering/ acquisition professionals

SV-AC-1

Attempting access to an access-controlled system resulting in unauthorized access

ID: SV-AC-1

Category: Crypto

CAPEC #: 20 | 21 | 94 | 102 | 114 | 115 | 161 | 180 | 248 | 463 | 594 | 616

NIST Rev5 Control Tag Mapping: IA-5(7) | SI-10(3) | AC-2(11) | AC-3(10) | AU-3(1) | IA-5 | IA-7 | SC-10 | SC-12 | SC-12(1) | SC-12(2) | SC-12(3) | SC-13 | SC-28(1) | SC-7 | SC-7(11) | SC-7(18) | AC-17(10) | SI-10 | SI-10(5) | AC-17(1) | AC-17(2) | AC-18(1)

Lowest Threat Tier to Create Threat Event: III

Notional Risk Rank Score: 25.0

Tied to CAPECs, NIST Controls, etc.

Sources

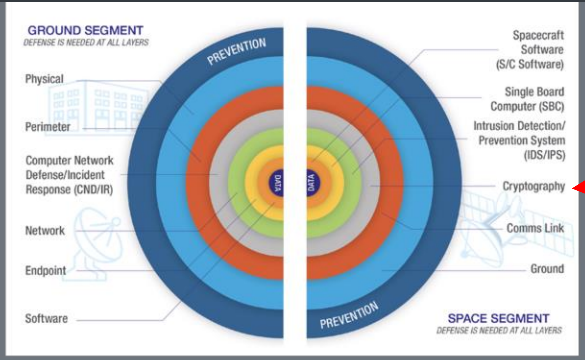
- CCSDS Threat Green Book
- CENTRA Volume I - Cyber Content of Satellites
- Cybersecurity for Space: Protecting the Final Frontier

High-Level Requirements

The spacecraft shall protect the commanding capability from intrusion.

Low-Level Requirements

Requirement	Rationale/Additional Guidance/Notes
The spacecraft shall implement relay and replay-resistant authentication mechanisms for establishing a remote connection. {SV-AC-1,SV-AC-2} {IA-2(8)}	
The spacecraft shall uniquely identify and authenticate the ground station and other SVs before establishing a remote connection. {SV-AC-1,SV-AC-2} {IA-3,IA-4,AC-17(10)}	This could be performed using comm ... the Program can update. The goal is s ... nflicts arise,
The spacecraft shall provide the capability to restrict command lock based on geographic location of ground stations. {SV-AC-1} {AC-2(11)}	Authorization can include embedding ... location, expected range of receive po ... against expected values. ... emitter ... ncrements
The spacecraft shall authenticate the ground station (and all commands) and other SVs before establishing remote connections using bidirectional authentication that is cryptographically based. {SV-AC-1,SV-AC-2} {IA-3(1),IA-4,IA-7,AC-17(10),AC-17(2),SC-7(11),AC-18(1)}	
The spacecraft shall not employ a mode of operations where cryptography on the TT&C link can be disabled (i.e., crypto-bypass mode). {SV-AC-1,SV-CF-1,SV-CF-2} {AC-3(10)}	
The spacecraft shall terminate the connection associated with a communications session at the end of the session or after [TBD minutes] of inactivity. {SV-AC-1} {SC-10}	



Space Segment		
DiD Layer	DiD Sub-Layer	Implementation Goal
Crypto	NSA Type-1	A Type 1 product is a device or system certified by the NSA for cryptographically securing confidentiality of classified U.S. Government information. Type-1 is usually only applicable to National Security Space missions. The term "Type 1" also refers to any cryptographic algorithm (or "Suite," as NSA refers to them) that has been approved by NSA for use within Type 1 equipment.
	Authentication (w/o Encryption)	Authentication, integrity, and the anti-replay function on the space communication link when data confidentiality is not required. Authentication for spacecraft commands provides assurance that the spacecraft can only be controlled/commanded by an authorized control center.
	Encryption (non-Type-1 w/o Authentication)	Provides data confidentiality but no authentication or integrity. Encryption primitives transform a block of plaintext data into ciphertext data. Encryption-only for a particular use case does not protect against malicious manipulation of data.
	Authenticated Encryption (non-Type-1)	Combination of encryption and authentication, thus, providing data confidentiality, data integrity, authentication, and anti-replay function. Authenticated encryption algorithms combine authentication and encryption algorithms with a single cryptographic key and algorithm.
	Crypto Bypass	Crypto bypass is completely disabled. All communication is properly encrypted.

Tied to Defense in Depth Model Too – Clickable menu for each layer describing recommended defenses/ countermeasures

Threats to Space Systems

This page contains spacecraft threats, vulnerabilities, and ground-based TTPs. The below generic threat library, as identified in TOR 2021-01333 REV A, was created by interviewing subject matter experts and reviewing many publications for threats, vulnerabilities, requirements, and security principles. Engineers can leverage this generic threat library to help identify likely threats that will drive the security requirements baseline. Space systems will likely have additional threats to consider, but the below depiction is a starting point for generating a security baseline. The below table establishes a library of layer-based threats and vulnerabilities using Aerospace's Defense-in-Depth model. The threats have unique identifiers denoted which have been cross referenced to the SPARTA matrix TTPs as well. This integration provides a method for leveraging the TOR 2021-01333 threat to requirement work within the context of SPARTA TTPs. In addition to the spacecraft information, there is also a table that maps TTPs for the ground segment using the ATT&CK Enterprise matrix. Select the View Threats to Ground button for more information.

View Threats to Space | View Threats to Ground

Data

- SV-AC-3 Compromised master keys or any encryption key
- SV-CF-2 Eavesdropping (RF and proximity)
- SV-IT-2 Unauthorized modification or corruption of data
- SV-MA-2 Heaters and flow valves of the propulsion subsystem are controlled by electric signals so cyberattacks against these signals could cause propellant lines to freeze, lock valves, waste propellant or even put in de-orbit or unstable spinning

S/C Software

- SV-AV-4 Attacking the scheduling table to affect tasking
- SV-IT-5 Onboard control procedures (i.e., ATS/RTS) that execute a scripts/sets of commands
- SV-MA-3 Attacks on critical software subsystems Attitude Determination and Control (AD&C) subsystem determines and controls the orientation of the satellite. Any cyberattack that could disrupt some portion of the control loop - sensor data, computation of control commands, and receipt of the commands would impact operations Telemetry, Tracking and Commanding (TT&C) subsystem provides interface between satellite and ground system. Computations occur within the RF portion of the TT&C subsystem, presenting cyberattack vector Command and Data Handling (C&DH) subsystem is the brains of the satellite. It interfaces with other subsystems, the payload, and the ground. It receives, validate, decodes, and sends commands to other subsystems, and it receives, processes, formats, and routes data for both the ground and onboard computer. C&DH has the most cyber content and is likely the biggest target for cyberattack. Electrical Power Subsystem (EPS) provides, stores, distributes, and controls power on the satellite. An attack on EPS could disrupt, damage, or destroy the satellite.
- SV-SP-1 Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, etc. in the FSW.
- SV-SP-3 Introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, keylogger, rootkit, or Trojan Horse
- SV-SP-6 Software reuse, COTS dependence, and standardization of onboard systems using building block approach with addition of open-source technology leads to supply chain threat
- SV-SP-9 On-orbit software updates/upgrades/patches/direct memory writes. If TT&C is compromised or MOC or even the developer's environment, the risk exists to do a variation of a supply chain attack where after it is in orbit you inject malicious code

SBC/Processor/Bus

- SV-AC-5 Proximity operations (i.e., grappling satellite)
- SV-AC-6 Three main parts of S/C. CPU, memory, I/O interfaces with parallel and/or serial ports. These are connected via busses (i.e., 1553) and need segregated. Supply chain attack on CPU (FPGA/ASICs), supply chain attack to get malware burned into memory through the development process, and rogue RTs on 1553 bus via hosted payloads are all threats. Security or fault management being disabled by non-mission critical or payload; fault injection or MiTM into the 1553 Bus - China has developed fault injector for 1553 - this could be a hosted payload attack if payload has access to main 1553 bus; One piece of FSW affecting another. Things are not containerized from the OS or FSW perspective;
- SV-AC-8 Malicious Use of hardware commands - backdoors / critical commands
- SV-AV-2 Satellites base many operations on timing especially since many operations are automated. Cyberattack to disrupt timing/timers could affect the vehicle (Time Jamming / Time Spoofing)
- SV-AV-3 Affect the watchdog timer onboard the satellite which could force satellite into some sort of recovery mode/protocol
- SV-AV-8 Clock synchronization attack for Spacewire. Since terminals in a distributed system are driven by independent clocks, the clock sync performance is one of the most important indexes in a networked system.
- SV-IT-3 Compromise boot memory
- SV-IT-4 Cause bit flip on memory via single event upsets
- SV-MA-8 Payload (or other component) is told to constantly sense or emit or run whatever mission it had to the point that it drained the battery constantly / operated in a loop at maximum power until the battery is depleted.

IDS/IPS

- SV-AV-5 Using fault management system against you. Understanding the fault response could be leveraged to get satellite in vulnerable state. Example, safe mode with crypto bypass, orbit correction maneuvers, affecting integrity of TLM to cause action from ground, or some sort of RPO to cause S/C to go into safe mode;
- SV-AV-6 Complete compromise or corruption of running state
- SV-DCO-1 Not knowing that you were attacked, or attack was attempted
- SV-MA-5 Not being able to recover from cyberattack

Crypto

- SV-AC-1 Attempting access to an access-controlled system resulting in unauthorized access
- SV-AC-2 Replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction
- SV-CF-1 Tapping of communications links (wireline, RF, network) resulting in loss of confidentiality; Traffic analysis to determine which entities are communicating with each other without being able to read the communicated information
- SV-CF-4 Adversary monitors for safe-mode indicators such that they know when satellite is in weakened state and then they launch attack
- SV-IT-1 Communications system spoofing resulting in denial of service and loss of availability and data integrity

Comms Link

- SV-AC-7 Weak communication protocols. Ones that don't have strong encryption within it
- SV-AV-1 Communications system jamming resulting in denial of service and loss of availability and data integrity

Ground

- SV-MA-7 Exploit ground system and use to maliciously to interact with the spacecraft

Prevention

- SV-AC-4 Masquerading as an authorized entity in order to gain access/Insider Threat
- SV-AV-7 The TT&C is the lead contributor to satellite failure over the first 10 years on-orbit, around 20% of the time. The failures due to gyro are around 12% between year one and 6 on-orbit and then ramp up starting around year six and overtake the contributions of the TT&C subsystem to satellite failure. Need to ensure equipment is not counterfeit and the supply chain is sound.
- SV-CF-3 Knowledge of target satellite's cyber-related design details would be crucial to inform potential attacker - so threat is leaking of design data which is often stored Unclass or on contractors' network
- SV-MA-1 Space debris colliding with the spacecraft
- SV-MA-4 Not knowing what your crown jewels are and how to protect them now and in the future.
- SV-MA-6 Not planning for security on SV or designing in security from the beginning
- SV-SP-10 Compromise development environment source code (applicable to development environments not covered by threat SV-SP-1, SV-SP-3, and SV-SP-4).
- SV-SP-2 Testing only focuses on functional requirements and rarely considers end to end or abuse cases
- SV-SP-4 General supply chain interruption or manipulation
- SV-SP-5 Hardware failure (i.e., tainted hardware) {ASIC and FPGA focused}

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Threats to Ground Systems

Aerospace analyzed each TTP from the ATT&CK for Enterprise matrix to map the TTP to Aerospace's Defense-in-Depth (DiD) model for the ground segment. The goal of this analysis was to bucket the TTPs into each layer, similar to the work performed on the spacecraft in TOR 2021-01333. The below table provides a mechanism at each layer to understand the TTPs a threat actor may leverage against that layer. Additionally, this analysis provides a mechanism to understand the best place for mitigations and detections. Clicking the individual TTP link will redirect to the ATT&CK for Enterprise entry that contains additional information (mitigations, detections, procedures, etc.) from ATT&CK. In addition to the ATT&CK matrix, there has also been work performed to map the TTP IDs to NIST RMF controls for more detailed mitigation elements. This work is hosted on GitHub at https://github.com/center-for-threat-informed-defense/attack-control-framework-mappings. There are spreadsheets, ATT&CK navigator overlays, etc. While understanding the mitigations is crucial, testing the detections or susceptibility of a ground segment element is equally important. An open-source resource has been published that enable automation of testing many of the ATT&CK TTPs. These "atomics" are tests broken down by TTP ID which will enable groups to test their ground system implementation for prevention and detection capability. This can be viewed at https://github.com/redcanaryco/atomic-red-team/tree/master/atomics

View Threats to Space | View Threats to Ground

Data	Ground Software Software	Endpoint	Network	CND/IR	Perimeter	Physical	Prevention
T1119 - Automated Collection	T1554 - Compromise Client Software Binary	T1548 - Abuse Elevation Control Mechanism	T1557 - Adversary-in-the-Middle	T1595 - Active Scanning	T1189 - Drive-by Compromise	T1052 - Exfiltration Over Physical Medium	T1583 - Acquire Infrastructure
T1619 - Cloud Storage Object Discovery	T1190 - Exploit Public-Facing Application	T1548.002 - Abuse Elevation Control Mechanism: Bypass User Account Control	T1557.002 - Adversary-in-the-Middle: ARP Cache Poisoning	T1595.001 - Active Scanning: Scanning IP Blocks	T1568.002 - Dynamic Resolution: Domain Generation Algorithms	T1052.001 - Exfiltration Over Physical Medium: Exfiltration over USB	T1583.005 - Acquire Infrastructure: Botnet
T1485 - Data Destruction	T1212 - Exploitation for Credential Access	T1548.004 - Abuse Elevation Control Mechanism: Elevated Execution with Prompt	T1557.003 - Adversary-in-the-Middle: DHCP Spoofing	T1595.002 - Active Scanning: Vulnerability Scanning	T1133 - External Remote Services	T1200 - Hardware Additions	T1583.002 - Acquire Infrastructure: DNS Server
T1486 - Data Encrypted for Impact	T1211 - Exploitation for Defense Evasion	T1548.001 - Abuse Elevation Control Mechanism: Setuid and Setgid	T1059.008 - Command and Scripting Interpreter: Network Device CLI	T1595.003 - Active Scanning: Wordlist Scanning	T1562.007 - Impair Defenses: Disable or Modify Cloud Firewall	T1091 - Replication Through Removable Media	T1583.001 - Acquire Infrastructure: Domains
T1565 - Data Manipulation	T1068 - Exploitation for Privilege Escalation	T1548.003 - Abuse Elevation Control Mechanism: Sudo and Sudo Caching	T1602 - Data from Configuration Repository	T1071 - Application Layer Protocol	T1566 - Phishing		T1583.004 - Acquire Infrastructure: Server
T1565.003 - Data Manipulation: Runtime Data Manipulation	T1210 - Exploitation of Remote Services	T1134 - Access Token Manipulation	T1602.002 - Data from Configuration Repository: Network Device Configuration Dump	T1071.004 - Application Layer Protocol: DNS	T1566.001 - Phishing: Spearphishing Attachment		T1583.003 - Acquire Infrastructure: Virtual Private Server
T1565.001 - Data Manipulation: Stored Data Manipulation	T1606.001 - Forge Web Credentials: Web Cookies	T1134.002 - Access Token Manipulation: Create Process with Token	T1602.001 - Data from Configuration Repository: SNMP (MIB Dump)	T1071.002 - Application Layer Protocol: File Transfer Protocols	T1566.002 - Phishing: Spearphishing Link		T1583.006 - Acquire Infrastructure: Web Services
T1530 - Data from Cloud Storage Object	T1036.001 - Masquerading: Invalid Code Signature	T1134.003 - Access Token Manipulation: Make and Impersonate Token	T1570 - Lateral Tool Transfer	T1071.003 - Application Layer Protocol: Mail Protocols	T1566.003 - Phishing: Spearphishing via Service		T1110.002 - Brute Force: Password Cracking
T1213.003 - Data from Information Repositories: Code Repositories	T1539 - Steal Web Session Cookie	T1134.004 - Access Token Manipulation: Parent PID Spoofing	T1601 - Modify System Image	T1071.001 - Application Layer Protocol: Web Protocols	T1090.002 - Proxy: External Proxy		T1586 - Compromise Accounts
T1213.001 - Data from Information Repositories: Confluence	T1195.001 - Supply Chain Compromise: Compromise Software Dependencies and Development Tools	T1134.005 - Access Token Manipulation: SID-History Injection	T1601.002 - Modify System Image: Downgrade System Image	T1020.001 - Automated Exfiltration: Traffic Duplication	T1204.001 - User Execution: Malicious Link		T1586.002 - Compromise Accounts: Email Accounts
T1213.002 - Data from Information Repositories: Sharepoint	T1195.002 - Supply Chain Compromise: Compromise Software Supply Chain	T1134.001 - Access Token Manipulation: Token Impersonation/Theft	T1601.001 - Modify System Image: Patch System Image	T1580 - Cloud Infrastructure Discovery	T1102.001 - Web Service: Dead Drop Resolver		T1586.001 - Compromise Accounts: Social Media Accounts
T1005 - Data from Local System	T1221 - Template Injection	T1531 - Account Access Removal	T1599 - Network Boundary Bridging	T1538 - Cloud Service Dashboard			T1584 - Compromise Infrastructure
T1039 - Data from Network Shared Drive	T1220 - XSL Script Processing	T1087 - Account Discovery	T1599.001 - Network Boundary Bridging: Network Address Translation Traversal	T1526 - Cloud Service Discovery			T1584.005 - Compromise Infrastructure: Botnet
T1025 - Data from Removable Media		T1087.004 - Account Discovery: Cloud Account	T1498 - Network Denial of Service	T1613 - Container and Resource Discovery			T1584.002 - Compromise Infrastructure: DNS Server
T1491 - Defacement		T1087.002 - Account Discovery: Domain Account	T1498.001 - Network Denial of Service: Direct Network Flood	T1136.003 - Create Account: Cloud Account			T1584.001 - Compromise Infrastructure: Domains
T1491.002 - Defacement: External Defacement		T1087.003 - Account Discovery: Email Account	T1498.002 - Network Denial of Service: Reflection Amplification	T1132 - Data Encoding			T1584.004 - Compromise Infrastructure: Server
T1561 - Disk Wipe		T1087.001 - Account Discovery: Local Account	T1040 - Network Sniffing	T1132.002 - Data Encoding: Non-Standard Encoding			T1584.003 - Compromise Infrastructure: Virtual Private Server
T1561.001 - Disk Wipe: Disk Content Wipe		T1098 - Account Manipulation		T1132.001 - Data Encoding: Standard Encoding			T1584.006 - Compromise Infrastructure: Web Services
T1561.002 - Disk Wipe: Disk Structure Wipe		T1098.001 - Account Manipulation: Additional Cloud Credentials		T1565.002 - Data Manipulation: Transmitted Data Manipulation			
T1568.001 - Dynamic Resolution:							