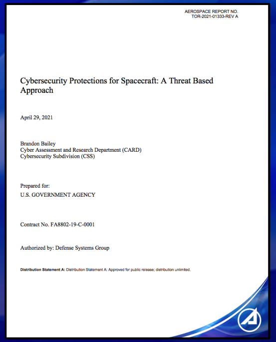
CYSAT 2023
Hacking Spacecraft using Space Attack Research & Tactic Analysis

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


AEROSPACE REPORT NO. TOR-2021-01333-REV A

Cybersecurity Protections for Spacecraft: A Threat Based Approach

April 29, 2021

Brandon Bailey
Cyber Assessment and Research Department (CARD)
Cybersecurity Subdivision (CSS)

Prepared for:
U.S. GOVERNMENT AGENCY

Contract No. FA8802-19-C-0001

Authorized by: Defense Systems Group

Papers:
- Defending Spacecraft in the Cyber Domain
- Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices
- Cybersecurity Protections for Spacecraft: A Threat Based Approach
- Protecting Space Systems from Cyber Attack

Presentations:
- DEF CON 2020: Exploiting Spacecraft
- DEF CON 2021: Unboxing the Spacecraft Software BlackBox Hunting for Vulnerabilities
- DEF CON 2022: Hunting for Spacecraft Zero Days using Digital Twins

https://aerospacecorp.medium.com/protecting-space-systems-from-cyber-attack-3db773aff368

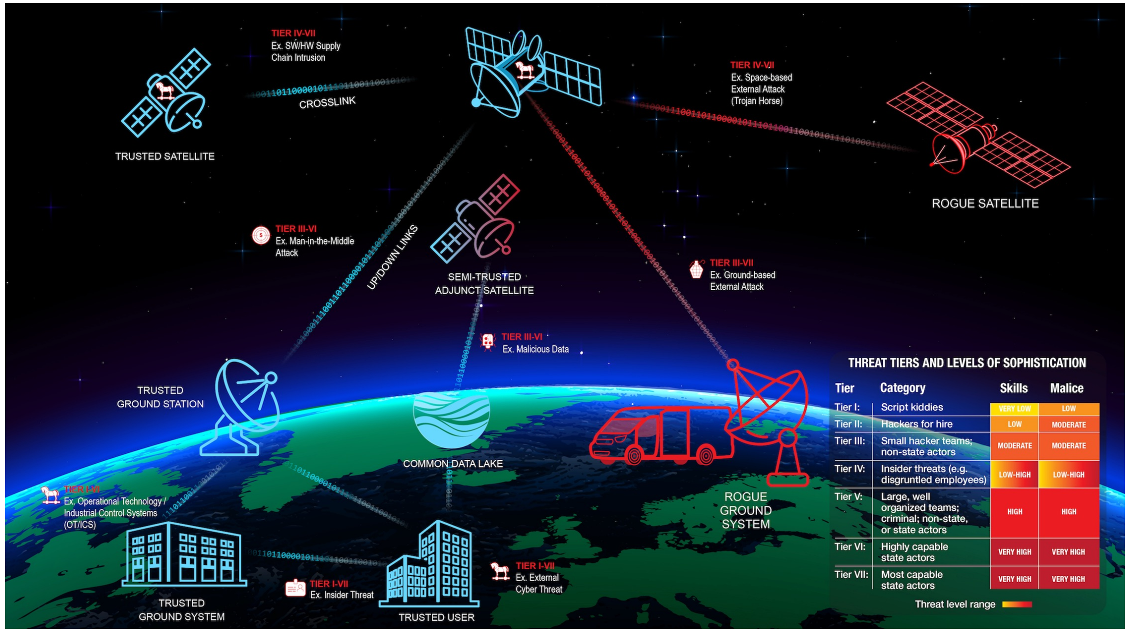
brandon.bailey@aero.org
240.521.4326 (c)

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

The Cybersecurity in Space Problem

- Traditional spacecraft/payload architectures, sub-systems, and supply chains were developed before current cyber threats were envisioned
- Traditionally, cybersecurity for DoD, civilian and commercial space systems has concentrated on the ground segment with minimal, if any, cyber protections onboard the SV/payload
  - *Encryption/Authentication, TRANSEC, COMSEC, and TEMPEST are typically the only controls (if any)*

- Aerospace is helping lead advancement in cybersecurity for the spacecraft and ground systems
  - *Many articles/publications identify problems, but few are solutions oriented*
    - Aerospace has had concerted effort on publishing information publicly to inform commercial & gov space sector
  - *One area is helping customers define the "right" requirements*
    - Defining the requirements using threats / tactics, techniques and procedures (TTPs) vice compliance requirements (ISO/ RMF baselines generated for traditional IT)
      - *TOR 2021-01333 REV A and now SPARTA provide resources to managers/developers/etc. to implement countermeasures to reduce cyber risk for space systems*



***blue lines* indicate normal expected communications/access**
***red lines* indicate communications from adversary's infrastructure directly**

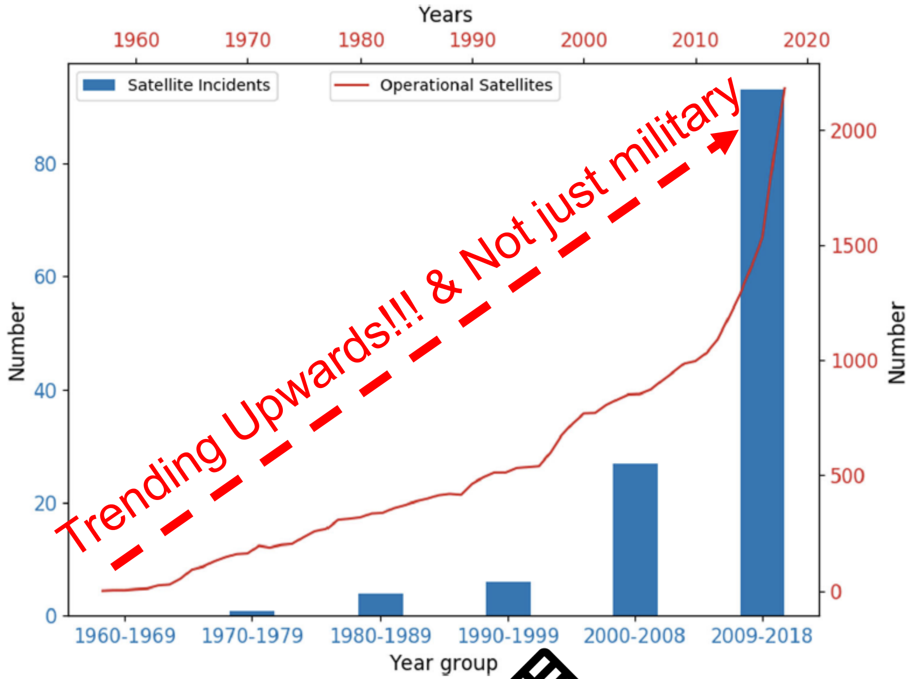
By defining the right cyber requirements/countermeasures, customers will be able reduce cyber risk for the space system

Example Cyber Incidents Against Space Systems

1. SPACE: Cybersecurity's Final Frontier, London Cybersecurity Report, *June 2015.*
2. Black Hat 2020: Satellite Comms Globally Open to $300 Eavesdropping Hack, Threatpost, Aug. 2020
3. Turla APT Group Abusing Satellite Internet Links, Threatpost, Sep. 2015
4. Network Security Breaches Plague NASA, Bloomberg, Nov 2008
5. Hackers Seized Control of Computers in NASA's Jet Propulsion Lab, WIRED, Mar. 2012
6. UT Austin Radio Radionavigation Laboratory
7. 2019 NASA OIG Report
8. Cyber security in New Space

Cyber security in New Space

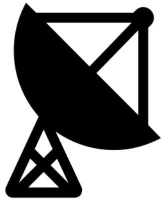
Fig. 6 Number of satellites attacks per year group is plotted on the bottom and left axes, and the number of operational satellites between 1958 and 2018 is plotted on the top and right axes



April 2005[4]: A rogue program penetrated NASA KSC networks, surreptitiously gathered data from computers in the Vehicle Assembly Building and removed that data through covert channels.

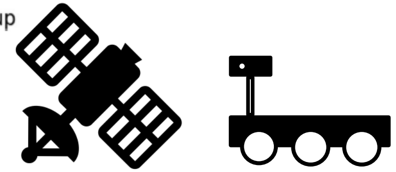
2011[5]: Cybercriminals managed to compromise the accounts of about 150 most privileged JPL users.

2018[7]: Weaknesses in JPL's system of security controls exploited; attacker moved undetected within multiple internal networks for about 10 months



Since 2007[3] several elite APT groups have been using — and abusing — satellite links to manage their operations — most often, their C&C infrastructure, for example, Turla.

Black Hat 2020[2]: Eavesdropping on Sat ISPs. Basically, ISP not protecting their links and it can be picked up easily.

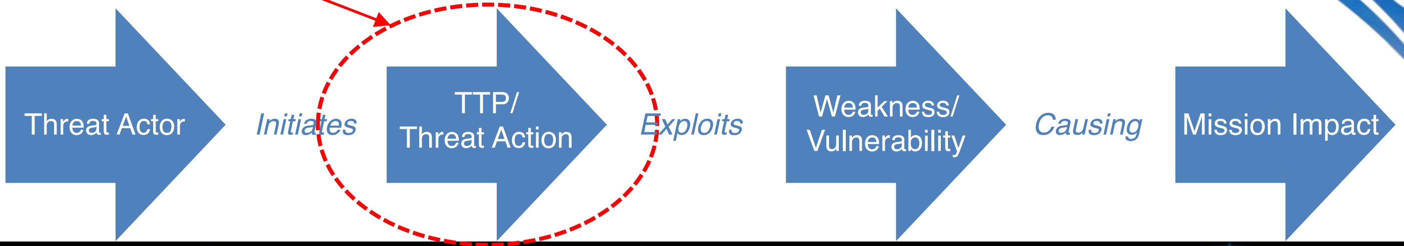


June/July 2008[1]: *Terra EOS AM-1/Landsat-7, a*ttempted satellite hijacking, hackers achieved all steps for remote command of satellite.

2013-2014:[6] UT Austin Radio-Navigation Lab conducts GPS spoofing for UAV control and navigation interruption.

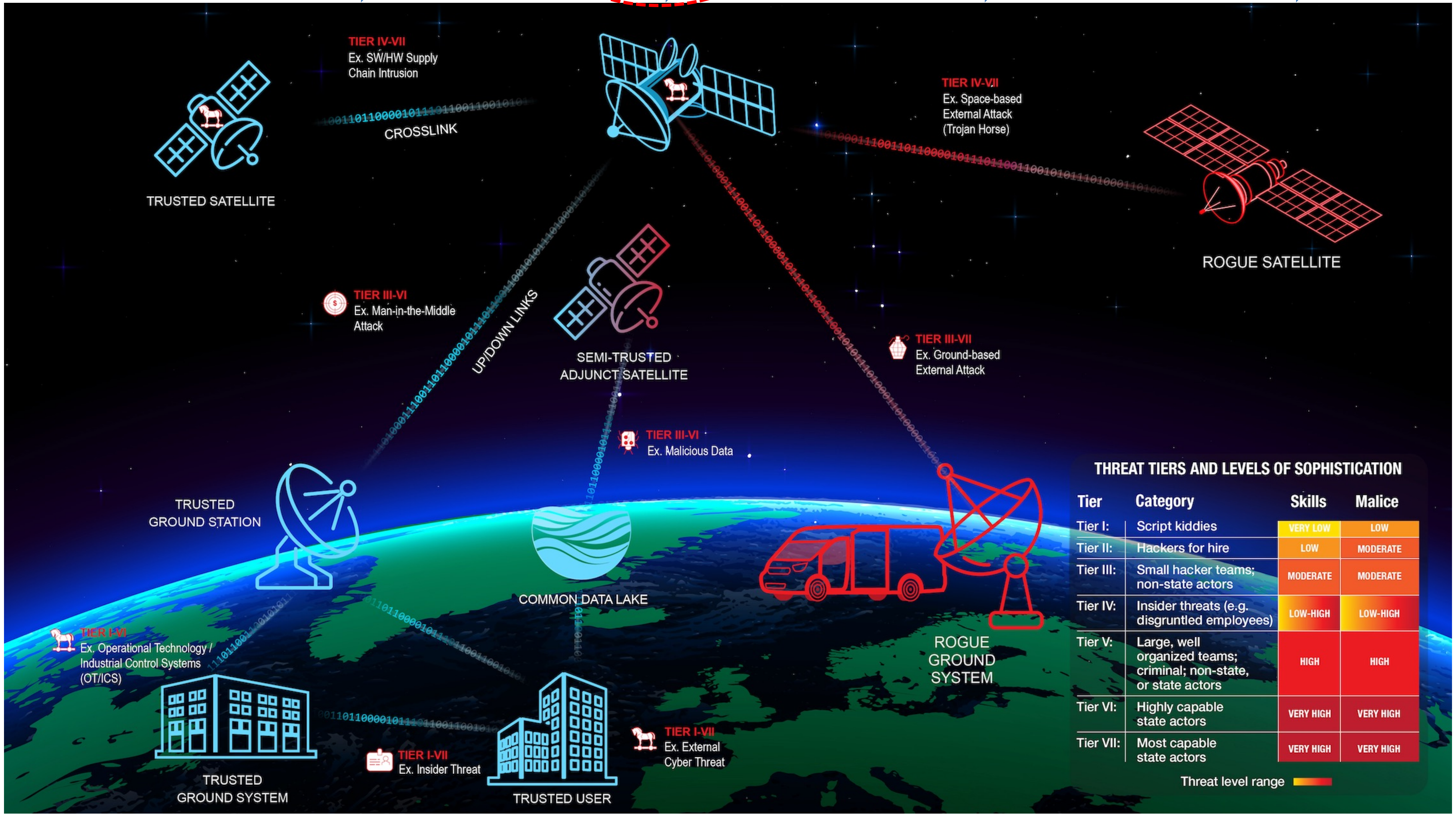
Attacks/TTPs

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



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*



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

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

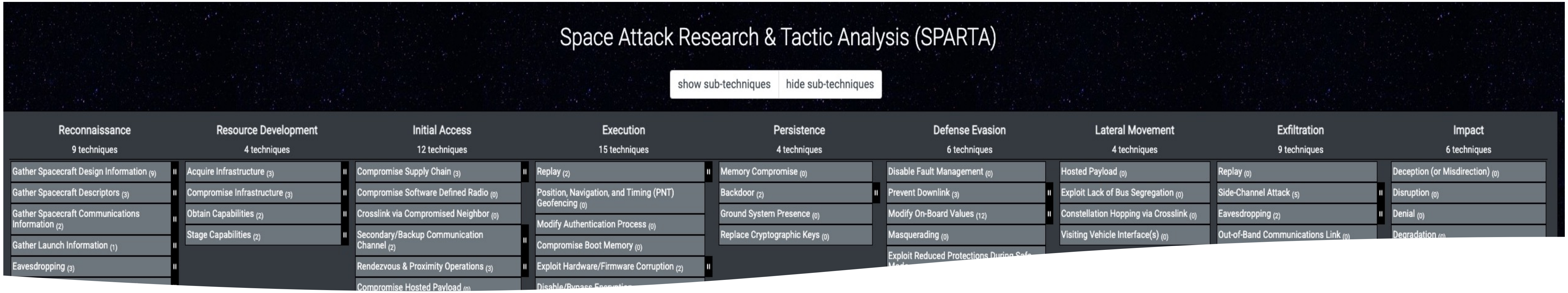
1 *Memorandum on Space Policy Directive – 5 Cybersecurity Principles for Space Systems, Sep 2020*

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

Filling the TTP Gap for Space

- Cybersecurity matrices are industry-standard tools and approaches for commercial and government users to navigate rapidly evolving cyber threats and vulnerabilities and outpace cyber threats
  - *They provide a critical knowledge base of adversary behaviors*
  - *Framework for adversarial actions across the attack lifecycle with applicable countermeasures*
- Current cybersecurity matrices (including MITRE ATT&CK) are limited to ground systems which lead to a gap!

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



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

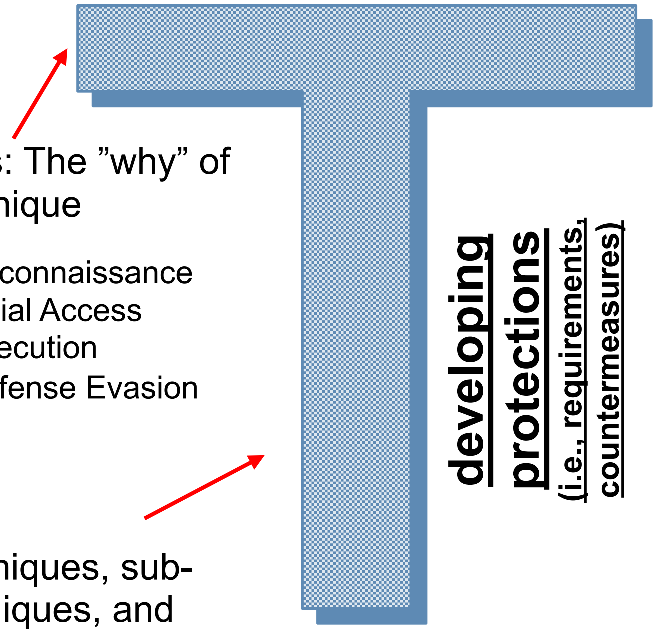
Space Attack Research & Tactic Analysis (SPARTA)

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 | 2022: 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)

understanding the threat



Tactics: The "why" of a technique

Reconnaissance
Initial Access
Execution
Defense Evasion
…

Techniques, sub-techniques, and procedures

Modify On-board values
Rogue Ground
Supply Chain
…

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

Building Spacecraft Attack Chains

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Blast from the Past

- Replay Attack from DefCon 2020
- Memory Injection Attack DefCon 2022

New Attacks

- Supply Chain Attack – Time bomb that executes command sequence 30 secs after boot
- Reaction Wheel Attack – Sending commands from rogue ground station due to no auth/encryption

Theoretical Attack Chain in Backup

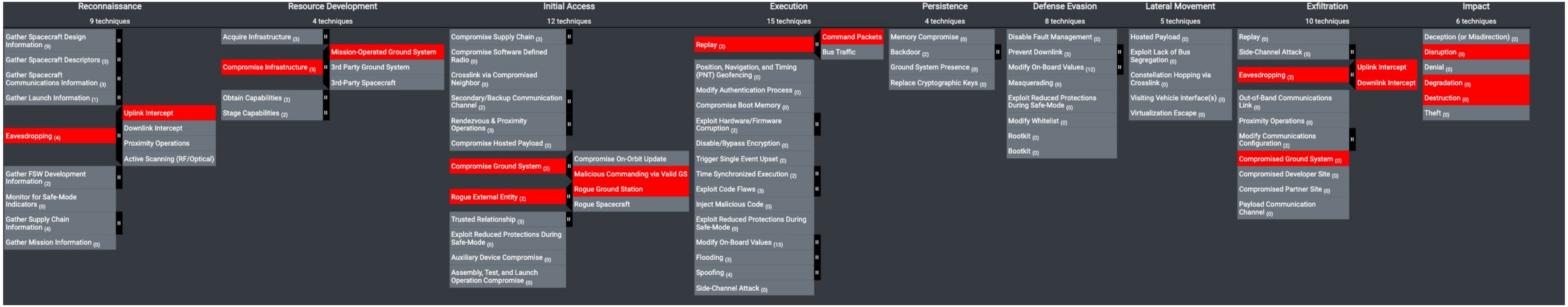
- PCspooF

SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

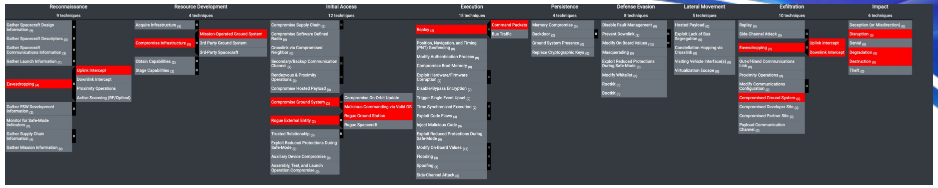
Example Attack Chains from the Past

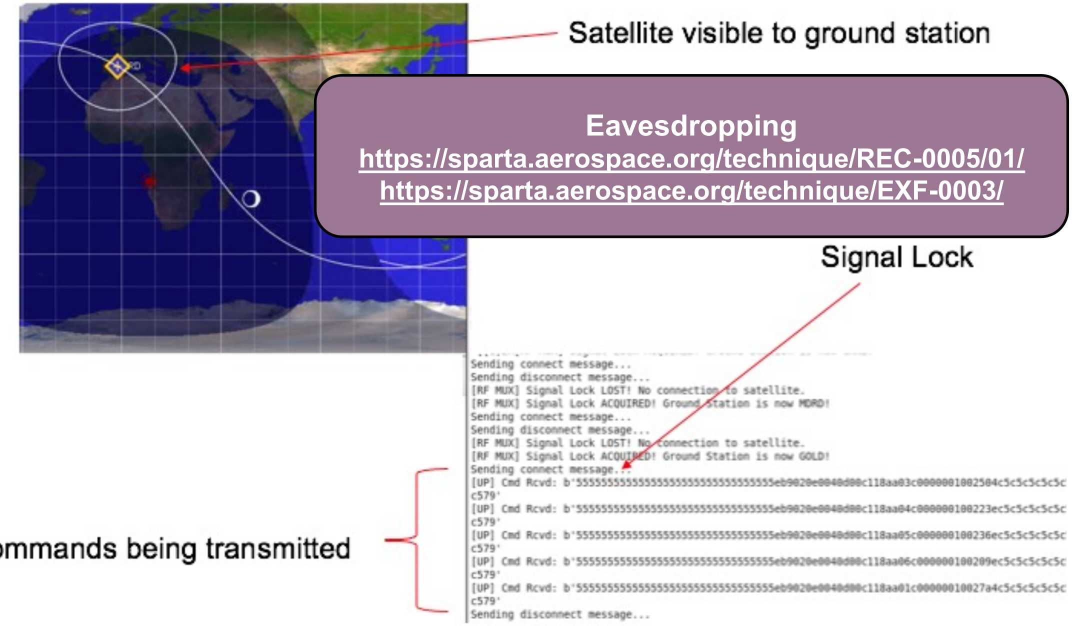
DefCon 2020 – Exploiting Spacecraft Example (https://www.youtube.com/watch?v=b8QWNiqTx1c)

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].



Replay Attack & Command Link Intrusion



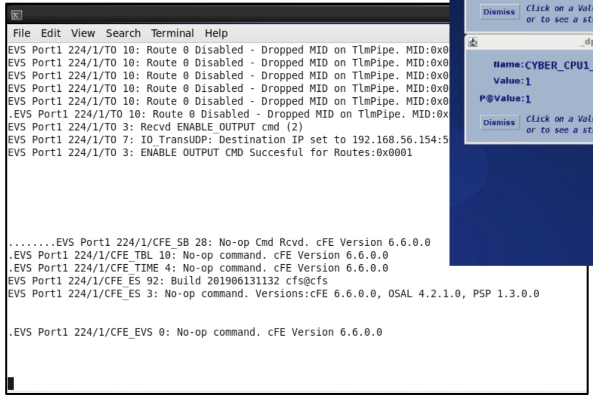


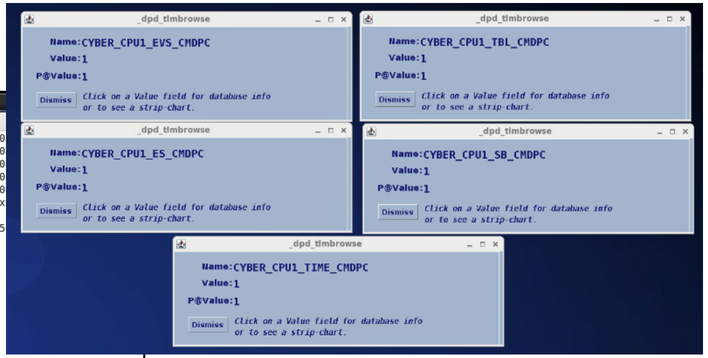
Satellite visible to ground station

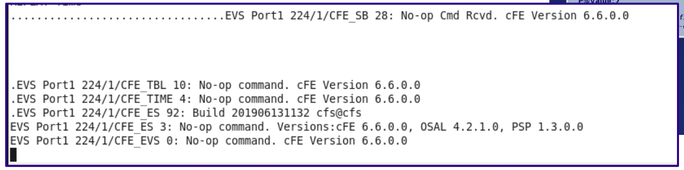
Eavesdropping
https://sparta.aerospace.org/technique/REC-0005/01/
https://sparta.aerospace.org/technique/EXF-0003/

Signal Lock

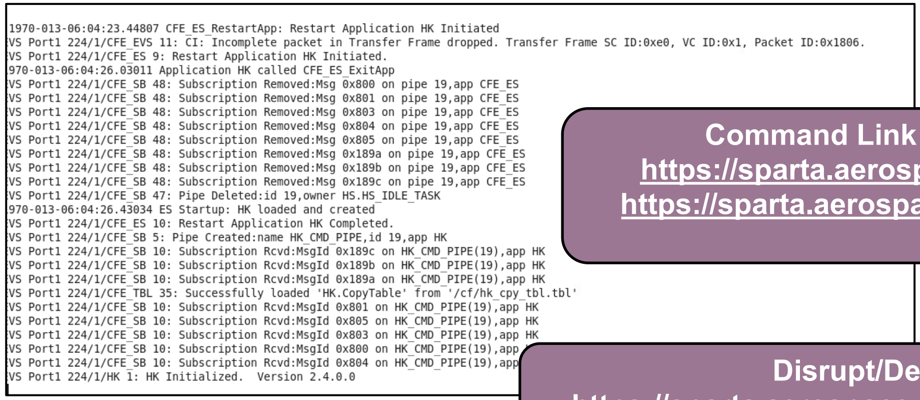
Commands being transmitted







Replay
https://sparta.aerospace.org/technique/EX-0001/



Command Link Intrusion from Ground
https://sparta.aerospace.org/technique/IA-0007/
https://sparta.aerospace.org/technique/IA-0008/01/

Disrupt/Degradation
https://sparta.aerospace.org/technique/IMP-0002/
https://sparta.aerospace.org/technique/IMP-0004/

Example SPARTA Countermeasures

Countermeasures

ID	Name	Description	NIST Rev5
CM0002	COMSEC	A component of cybersecurity to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. It is imperative to utilize 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.	AC-17(1) | AC-17(10) | AC-17(10) | AC-17(2) | AC-18(1) | AC-2(11) | AC-3(10) | IA-4(9) | IA-5 | IA-5(7) | IA-7 | SA-8(18) | SA-9(6) | SC-10 | SC-12 | SC-12(1) | SC-12(2) | SC-12(3) | SC-12(6) | SC-13 | SC-13(1) | SC-13(2) | SC-16(3) | SC-28(1) | SC-28(3) | SC-7 | SC-7(10) | SC-7(11) | SC-7(18) | SC-7(5) | SI-10 | SI-10(3) | SI-10(5) | SI-10(6) | SI-19(4) | SI-3(8)
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.	AC-17(10) | AC-17(10) | AC-17(2) | AC-18(1) | IA-3(1) | IA-4 | IA-4(9) | IA-7 | SA-8(15) | SA-8(9) | SC-16(2) | SC-32(1) | SC-7(11) | SI-14(3)
CM0033	Relay Protection	Implement relay and replay-resistant authentication mechanisms for establishing a remote connection or connections on the spacecraft bus.	AC-17(10) | AC-17(10) | IA-2(8) | IA-3 | IA-3(1) | IA-4 | IA-7 | SC-13 | SC-23 | SC-7 | SC-7(11) | SC-7(18) | SI-10 | SI-10(5) | SI-10(6) | SI-3(8)

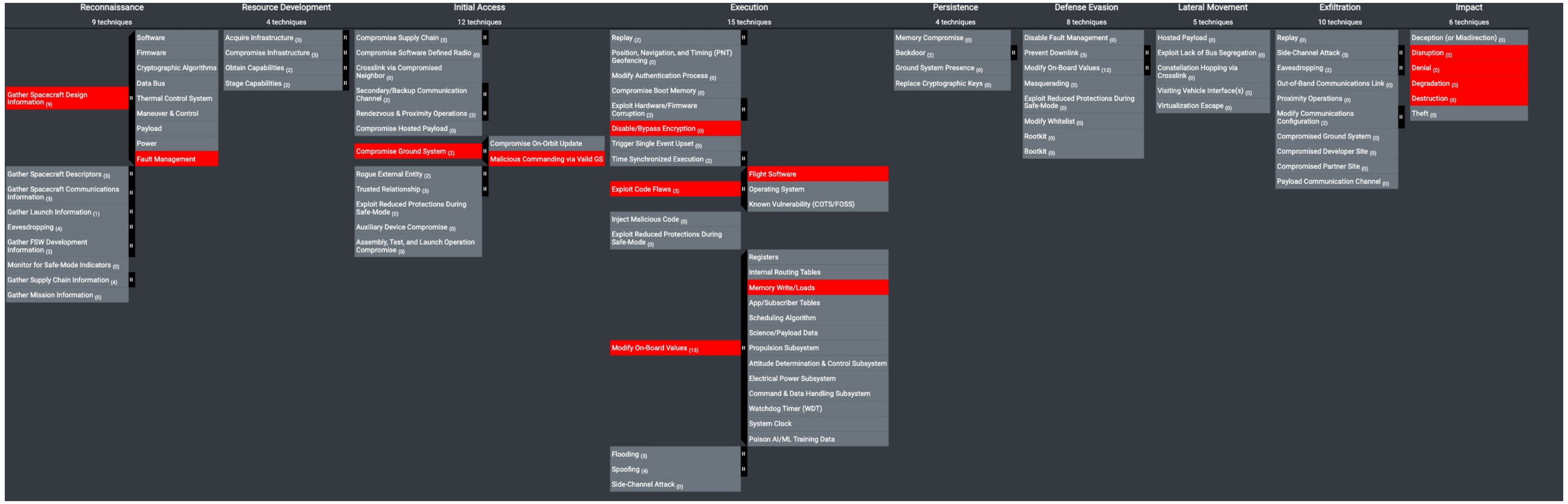
SPARTA
SPACE ATTACK RESEARCH & TACTIC ANALYSIS

Example Attack Chains from the Past

DefCon 2022 - Memory Manipulation Attack (https://www.youtube.com/watch?v=t_efCpd2PbM)

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].



Fuzzing Memory Addresses

Lots of Trial and Error

- Hardware design documentation reveals “features” of hardware design
  - *Can these features be leveraged for nefarious purposes?*
    - Creating faults, abusing functions, etc. from design docs are common TTPs when performing aggression on spacecraft technology
- Lots of debugging and reverse engineering later
  - *Setting breakpoints, working with registers, memory regions, etc.*
    - Digital twins come in extremely handy during this research
      - *See: Hunting for Spacecraft Zero Days using Digital Twins*
  - *Triggering exceptions and understanding what they mean*

```
Sending garbage to 0x3
KI2LoadVMBookmark() result: True
b'FED123$\xa4'
Timeout occurred!
Sending garbage to 0x3
KI2LoadVMBookmark() result: True
b'FED123$|'
Timeout occurred!
Sending garbage to 0x3
KI2LoadVMBookmark() result: True
b'FED123$`'
Exception occurred!
  Exception type: 1
Exception occurred!
  Exception type: 1
Timeout occurred!
Sending garbage t
KI2LoadVMBookmark
b'FED123$\x00'
Exception occurre
  Exception type:
```

```
Timeout occurred!
Inputting b'0x1
Timeout occurred!
Inputting b'0x1
Timeout occurred!
Inputting b'0x1
Timeout occurred!
Inputting b'0x1
Timeout occurred!
Inputting b'0x1
Timeout occurred!
Inputting b'0x1
Timeout occurred!
Inputting b'0x1
```

```
Sending garbage to 0x:
Exception occurred!
        PowerPC Exception 6: Alignment Exception
                Error Code: 262144
Exception occurred!
        PowerPC Exception 7: Program Exception
                Error Code: 0
Timeout occurred!
Sending garbage to 0x:
Exception occurred!
        PowerPC Exception 2: Machine Check
                Error Code: 0
Exception occurred!
        PowerPC Exception 2: Machine Check
                Error Code: 0
Timeout occurred!
Sending garbage to 0x:
Exception occurred!
        PowerPC Exception 2: Machine Check
                Error Code: 0
Exception occurred!
        PowerPC Exception 2: Machine Check
                Error Code: 0
Timeout occurred!
Sending garbage to 0x:
```

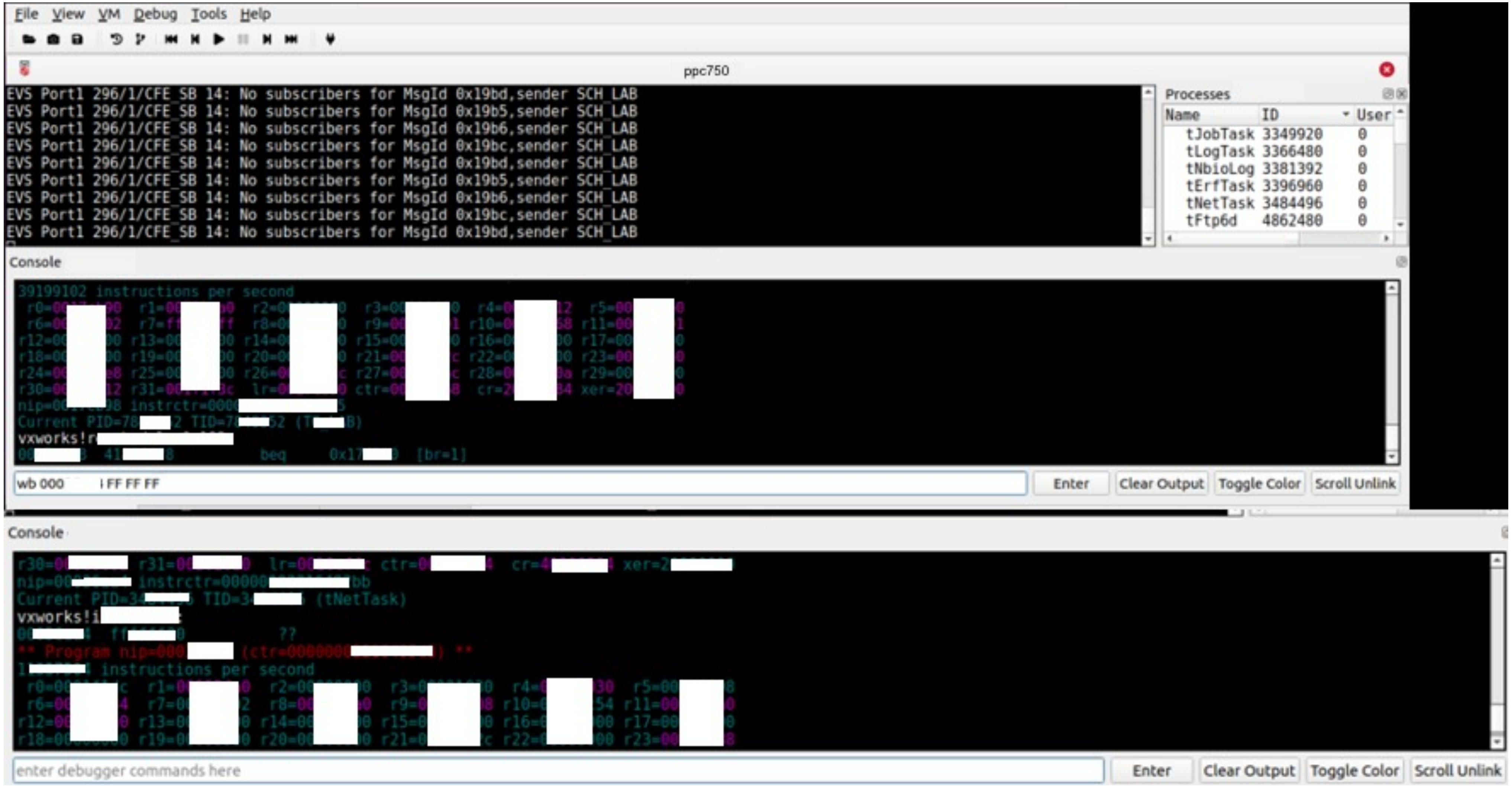
Table 6-2. Exceptions and Conditions—Overview

Exception Type	Vector Offset (hex)	Causing Conditions
Reserved	00000	—
System reset	00100	The causes of system reset exceptions are *implementation-dependent*. If the conditions that cause the exception also cause the processor state to be corrupted such that the contents of SRR0 and SRR1 are no longer valid or such that other processor resources are so corrupted that the processor cannot reliably resume execution, the copy of the RI bit copied from the MSR to SRR1 is *cleared*.
Machine check	00200	The causes for machine check exceptions are implementation-dependent, but typically these causes are related to conditions such as bus parity errors or attempting to access an invalid physical address. Typically, these exceptions are triggered by an input signal to the processor. Note that not all processors provide the same level of error checking. The machine check exception is disabled when MSR[ME] = 0. If a machine check exception condition exists and the ME bit is cleared, the processor goes into the checkstop state. If the conditions that cause the exception also cause the processor state to be corrupted such that the contents of SRR0 and SRR1 are no longer valid or such that other processor resources are so corrupted that the processor cannot reliably resume execution, the copy of the RI bit written from the MSR to SRR1 is cleared. (Note that physical address is referred to as real address in the architecture specification.)
DSI	00300	A DSI exception occurs when a data memory access cannot be performed for any of the reasons described in Section 6.4.3, "DSI Exception (0x00300)." Such accesses can be generated by load/store instructions, certain memory control instructions, and certain cache control instructions.
ISI	00400	An ISI exception occurs when an instruction fetch cannot be performed for a variety of reasons described in Section 6.4.4, "ISI Exception (0x00400)."
External interrupt	00500	An external interrupt is generated only when an external interrupt is pending (typically signalled by a signal defined by the implementation) and the interrupt is enabled (MSR[EE] = 1).
Alignment	00600	An alignment exception may occur when the processor cannot perform a memory access for reasons described in Section 6.4.6, "Alignment Exception (0x00600)." Note that an implementation is allowed to perform the operation correctly and not cause an alignment exception.

https://www.nxp.com/docs/en/user-guide/MPCFPE_AD_R1.pdf

Manually Invoking Crash – Post Fuzzing

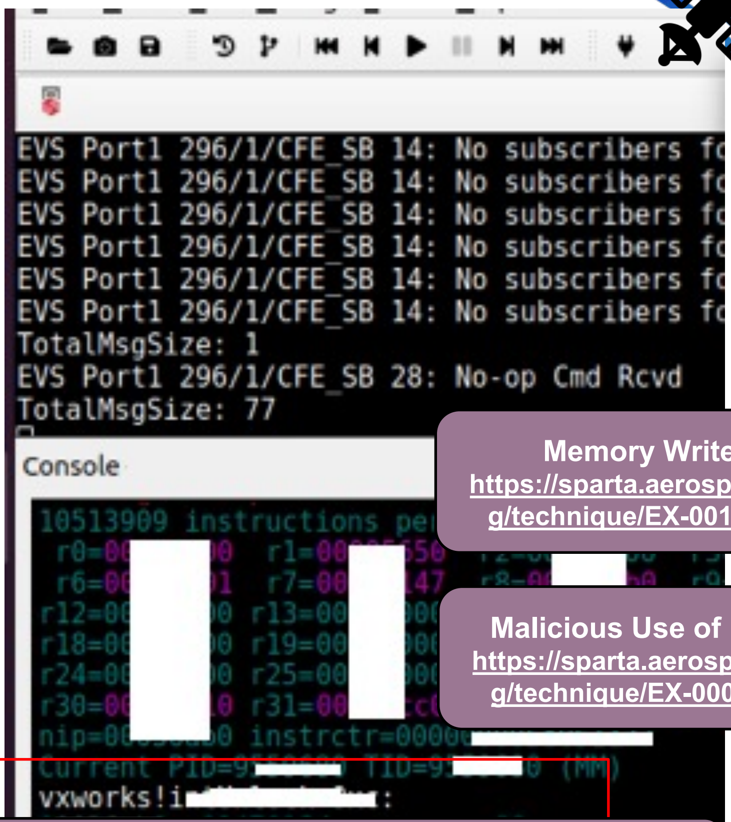
Confirming Input Results Provides Desired Reaction



Initiating the Crash from the Ground

Mapping the TTPs

- Sending No-Op followed by Magic Packet to crash the spacecraft processor
  - *This is where having direct memory access via the spacecraft FSW can be dangerous and must be protected*
    - The inherit trust between ground systems and spacecraft MUST be accounted for and better protections on-board the spacecraft are necessary moving forward
      - *Too many instances where the ground can issue legitimate commands to degrade/deny/destroy the spacecraft*
        - Must extend fault management to account for this truth



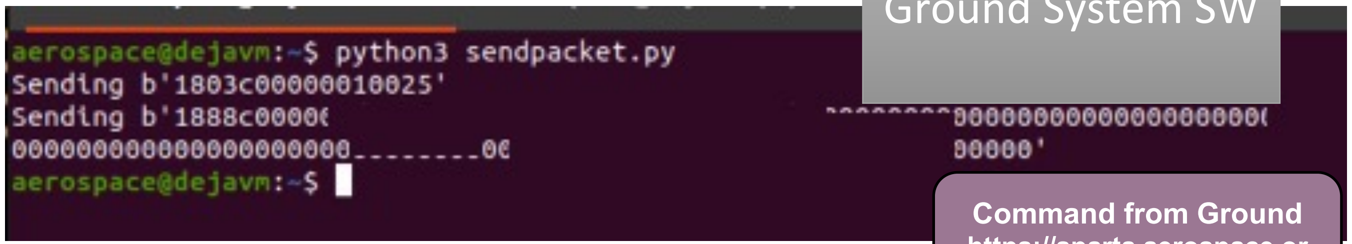
Memory Write
https://sparta.aerospace.org/technique/EX-0012/03/

Malicious Use of FSW
https://sparta.aerospace.org/technique/EX-0009/01/

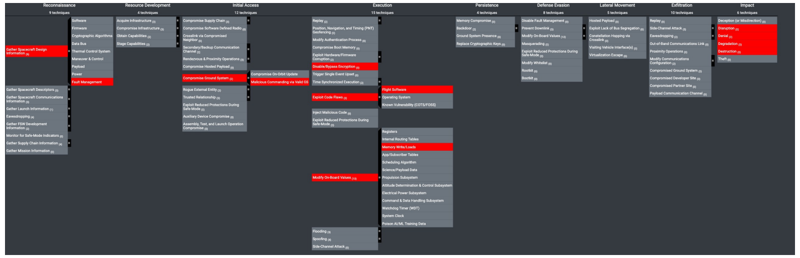
Space-Ground Link (UDP)

Disrupt/Denial
https://sparta.aerospace.org/technique/IMP-0002/
https://sparta.aerospace.org/technique/IMP-0003/

Ground System SW



Command from Ground
https://sparta.aerospace.org/technique/IA-0007/02/



Countermeasures

Example SPARTA Countermeasures

<table>
<tr><th>ID</th><th>Name</th><th>Description</th><th>NIST Rev5</th></tr>
<tr><td>CM0069</td><td>Process White Listing</td><td>Simple process ID whitelisting on the firmware level could impede attackers from instigating unnecessary processes which could impact the spacecraft</td><td>CM-7(5) | SI-10(5)</td></tr>
<tr><td>CM0032</td><td>On-board Intrusion Detection & Prevention</td><td>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 (initial access, execution, persistence, evasion, exfiltration, etc.) 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.</td><td>AU-14 | AU-2 | AU-3 | AU-3(1) | AU-4 | AU-4(1) | AU-5 | AU-5(2) | AU-5(5) | AU-6(1) | AU-6(4) | AU-8 | AU-9 | AU-9(2) | AU-9(3) | CA-7(6) | CM-11(3) | CP-10 | CP-10(4) | IR-4 | IR-4(11) | IR-4(12) | IR-4(14) | IR-4(5) | IR-5 | IR-5(1) | RA-10 | RA-3(4) | SA-8(21) | SA-8(22) | SA-8(23) | SC-16(2) | SC-32(1) | SC-5 | SC-5(3) | SC-7(10) | SC-7(9) | SI-10(6) | SI-16 | SI-17 | SI-3 | SI-3(8) | SI-4 | SI-4(1) | SI-4(10) | SI-4(11) | SI-4(13) | SI-4(16) | SI-4(17) | SI-4(2) | SI-4(23) | SI-4(24) | SI-4(25) | SI-4(4) | SI-4(5) | SI-6 | SI-7(17) | SI-7(8)</td></tr>
<tr><td>CM0042</td><td>Robust Fault Management</td><td>Ensure fault management system cannot be used against the spacecraft. Examples include: safe mode with crypto bypass, orbit correction maneuvers, affecting integrity of telemetry to cause action from ground, or some sort of proximity operation to cause spacecraft to go into safe mode. Understanding the safing procedures and ensuring they do not put the spacecraft in a more vulnerable state is key to building a resilient spacecraft.</td><td>CP-4(5) | SA-8(24) | SC-16(2) | SC-24 | SC-5 | SI-13 | SI-17</td></tr>
<tr><td>CM0044</td><td>Cyber-safe Mode</td><td>Provide the capability to enter the spacecraft into a configuration-controlled and integrity-protected state representing a known, operational cyber-safe state (e.g., cyber-safe mode). Spacecraft should enter a cyber-safe mode when conditions that threaten the platform are detected. Cyber-safe mode is an operating mode of a spacecraft during which all nonessential systems are shut down and the spacecraft is placed in a known good state using validated software and configuration settings. Within cyber-safe mode, authentication and encryption should still be enabled. The spacecraft should be capable of reconstituting firmware and software functions to pre-attack levels to allow for the recovery of functional capabilities. This can</td><td>CP-10 | CP-10(4) | CP-12 | CP-2(5) | IR-4 | IR-4(12) | IR-4(3) | SA-8(21) | SA-8(23) | SA-8(24) | SC-16(2) | SC-24 | SC-5 | SI-11 | SI-17 | SI-7(17)</td></tr>
</table>

Supply Chain Injection – Boot Sequence (RTS)

RTS001 loads after boot

3.4.5 Naming Conventions for RTSs

Because RTSs can be loaded at startup, the files for those RTSs must be in a predetermined location ~~(CFS SC Configuration Parameter SC_RTS_FILE_NAME)~~.

This location must be in non-volatile memory. Otherwise, the files would not exist upon a Power-On reset.

Also, the RTS table file must be named according to a specific convention (CFS SC Configuration Parameter SC_RTS_TABLE_NAME). The file name must start with the value of the (CFS SC Configuration Parameter SC_RTS_TABLE_NAME) platform configuration parameter.

Next, must be a three digit number indicating which RTS this table file is, and the last must be ".tbl". An example of this for RTS No.1, with SC_RTS_TABLE_NAME set to "RTS_TBL" would be: 'RTS_TBL001.tbl'.

In addition to the file naming convention, the name of the table contained within the table file should be the same as the file name, without the path or extension.

Remember to also have the application name prefixed to the name of the table. For the file 'RTS_TBL001.tbl', its table name should be 'SC.RTS_TBL001, if the name of the application is "SC".

2.2.7 RTS Tables

RTS tables are a sequence of Relative Time Sequence commands. The purpose of Relative Time Sequence commands is to be able to specify commands to be executed at a specific time *after* ("relative to") an ATS.

For Relative Time Command Sequence commands there is a field that represents the time in seconds that the command will *delay* before executing. This delay is relative to the time when the previous Relative Time Tagged Command (RTC) was executed. In the case of the first command of the sequence, this time is relative to when the sequence was started.

More details of timing and format for RTS tables are shown in Chapter 3.

RTS001

```
/*
** RTS Table Data
*/
uint16 RTS_Table001[SC_RTS_BUFF_SIZE] =
{
/* cmd time,  <---------------------------- cmd pkt primary header ---------------------------->    <----- cmd pkt 2nd header ---->    <-- opt data --->
  1,          CFE_MAKE_BIG16(DS_CMD_MID),          CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(5),     CFE_MAKE_BIG16(DS_SET_APP_STATE_CC),     0x0001, 0x0000, /
  1,          CFE_MAKE_BIG16(TO_LAB_CMD_MID),      CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(21),    CFE_MAKE_BIG16(TO_DEBUG_ENABLE_CC),      0x0031, 0x3237, 0
  1,          CFE_MAKE_BIG16(SAMPLE_APP_CMD_MID),  CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(1),     CFE_MAKE_BIG16(SAMPLE_APP_NOOP_CC),      // Sample Instrum
  5,          CFE_MAKE_BIG16(LC_CMD_MID),          CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(5),     CFE_MAKE_BIG16(LC_SET_LC_STATE_CC),      0x0001, 0x0000, /

};
```

```
** RTS Table Data
*/
uint16 RTS_Table001[SC_RTS_BUFF_SIZE] =
{
/* cmd time,  <---------------------------- cmd pkt primary header ---------------------------->    <----- cmd pkt 2nd header ---->    <-- opt data ---> */
  1,          CFE_MAKE_BIG16(DS_CMD_MID),          CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(5),     CFE_MAKE_BIG16(DS_SET_APP_STATE_CC),     0x0001, 0x0000, // Enable DS
  1,          CFE_MAKE_BIG16(TO_LAB_CMD_MID),      CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(21),    CFE_MAKE_BIG16(TO_DEBUG_ENABLE_CC),      0x0031, 0x3237, 0x2E30, 0x2E30, 0x2E31, 0x
  1,          CFE_MAKE_BIG16(SAMPLE_CMD_MID),      CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(1),     CFE_MAKE_BIG16(SAMPLE_APP_NOOP_CC),      // Sample Instrument NOOP
  5,          CFE_MAKE_BIG16(LC_CMD_MID),          CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(5),     CFE_MAKE_BIG16(LC_SET_LC_STATE_CC),      0x0001, 0x0000, // Enable LC
  6,          CFE_MAKE_BIG16(0x18A9),          CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(1),     CFE_MAKE_BIG16(0x0000),          // SC NOOP - Test Command
  7,          CFE_MAKE_BIG16(0x1806),              CFE_MAKE_BIG16(PKT_FLAGS), CFE_MAKE_BIG16(3),     CFE_MAKE_BIG16(0x0200),     0x0002 //Reset ATTACK
```

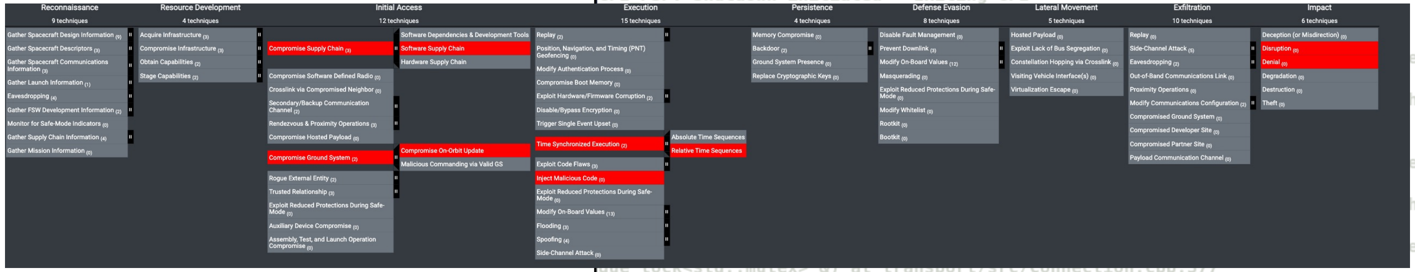
Compromise Supply Chain: Software Supply Chain
https://sparta.aerospace.org/technique/IA-0001/02/

```
EVS Port1 42/1/SC 73: RTS Number 001 Started
EVS Port1 42/1/SCH 21: Major Frame Sync too noisy (Slot 1). Disabling synchronization.
EVS Port1 42/1/TO_LAB 3: TO telemetry output enabled for IP 1
EVS Port1 42/1/SAMPLE 11: SAMPLE: NOOP command received
EVS Port1 42/1/LC 28: Set LC state command: new state = 1
EVS Port1 42/1/SC 52: No-op command. Version 2.5.0.0
EVS Port1 42/1/SC 86: RTS 001 Execution Completed
2000-001-00:00:24.26000 POWERON RESET called from CFE_ES_ResetCFE (Commanded).
CFE_PSP: Exiting cFE with POWERON Reset status.
CFE_PSP: Critical Data Store Shared memory segment removed
Reset Area Shared memory segment removed
User Reserved Area Shared memory segment removed

CFE_PSP: Shutdown initiated - Exiting cFE
ed to receive message, connection was shutdown in NosEngine::Transport::Connection::process_stop(std::uni
ht exception while receiving message, will stop receiving, message connection was shutdown, before async
ed to receive message, connection was shutdown in NosEngine::Transport::Connection::process_stop(std::uni
ht exception while receivin
ed to receive message, conn
que_lock<std::mutex> &) at transport/src/connection.cpp:377
2023-03-27 12:55:37.649964 [ ERROR ] NosEngine.Common - receive operator caught exception while receiving
receive message started
```

Reboot command but could be "anything" – like reaction wheels?

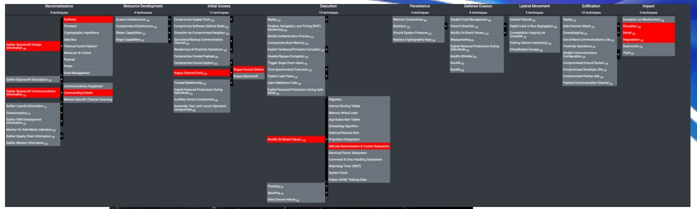
Inject Malicious Code & Time Synchronized Execution: Relative Time Sequences
https://sparta.aerospace.org/technique/EX-0010/
https://sparta.aerospace.org/technique/EX-0008/02/

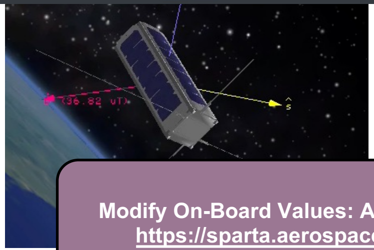


Disrupt/Denial
https://sparta.aerospace.org/technique/IMP-0002/
https://sparta.aerospace.org/technique/IMP-0003/

Rogue Ground Station – Attacking Reaction Wheel

Spinning a CubeSat Uncontrollably





Modify On-Board Values: Attitude Determination & Control
https://sparta.aerospace.org/technique/EX-0012/08/

- Many CubeSats do not implement strong, sometimes any, authentication / encryption – therefore, can could be vulnerable to command link intrusion from Rogue Ground Station
- Requires reconnaissance on spacecraft

Gather Spacecraft Design Information: Software
https://sparta.aerospace.org/technique/REC-0001/01/

Gather Spacecraft Communications Information: Commanding Details
https://sparta.aerospace.org/technique/REC-0003/02/

Rogue Ground System SW

1992c000000303001400

Command Link Intrusion from Rogue Ground
https://sparta.aerospace.org/technique/IA-0008/01/

- This attack creates a CCSDS frame to send to spacecraft from a rogue ground station

```
0000000 0d0a 0a0d 0060 0000 3c4d 1a2b 0001 0000
0000010 ffff ffff ffff ffff 0004 003a 6445 7469
0000020 6163 2070 5728 7269 7365 6168 6b72 2029
0000030 2e33 2e32 2033 4728 7469 7620 2e33 2e32
0000040 2033 6170 6b63 6761 6465 6120 2073 2e33
0000050 2e32 2d33 2931 0000 0000 0000 0060 0000
0000060 0001 0000 0014 0000 0001 0000 0000 0004
0000070 0014 0000 0006 0000 0054 0000 0000 0000
0000080 f7a5 0005 23d7 faa0 0032 0000 0032 0000
0000090 0000 0000 0000 0000 0000 0000 0008 0045
00000a0 2400 58a6 0040 1140 6e96 007f 0100 007f
00000b0 0100 acbc 9413 1000 23fe 9219 00c0 0300
00000c0 0003 0014 0054 0000
00000c8
```

https://github.com/nasa/nos3

Example SPARTA Countermeasures

Countermeasures

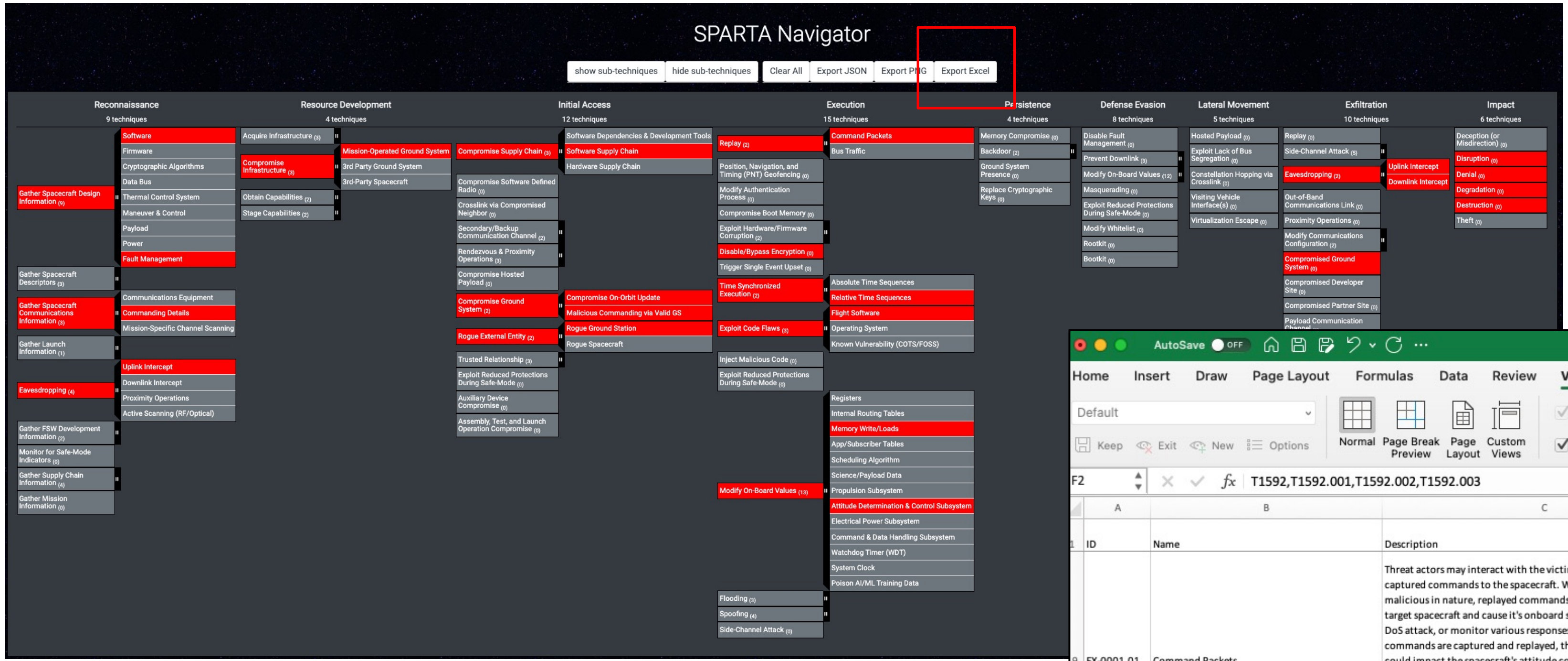
<table>
<tr><th>ID</th><th>Name</th><th>Description</th><th>NIST Rev5</th></tr>
<tr><td>CM0002</td><td>COMSEC</td><td>A component of cybersecurity to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. It is imperative to utilize 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.</td><td>AC-17(1) | AC-17(10) | AC-17(10) | AC-17(2) | AC-18(1) | AC-2(11) | AC-3(10) | IA-4(9) | IA-5 | IA-5(7) | IA-7 | SA-8(18) | SA-9(6) | SC-10 | SC-12 | SC-12(1) | SC-12(2) | SC-12(3) | SC-12(6) | SC-13 | SC-13(1) | SC-13(2) | SC-16(3) | SC-28(1) | SC-28(3) | SC-7 | SC-7(10) | SC-7(11) | SC-7(18) | SC-7(5) | SI-10 | SI-10(3) | SI-10(5) | SI-10(6) | SI-19(4) | SI-3(8)</td></tr>
<tr><td>CM0031</td><td>Authentication</td><td>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.</td><td>AC-17(10) | AC-17(10) | AC-17(2) | AC-18(1) | IA-3(1) | IA-4 | IA-4(9) | IA-7 | SA-8(15) | SA-8(9) | SC-16(2) | SC-32(1) | SC-7(11) | SI-14(3)</td></tr>
<tr><td>CM0033</td><td>Relay Protection</td><td>Implement relay and replay-resistant authentication mechanisms for establishing a remote connection or connections on the spacecraft bus.</td><td>AC-17(10) | AC-17(10) | IA-2(8) | IA-3 | IA-3(1) | IA-4 | IA-7 | SC-13 | SC-23 | SC-7 | SC-7(11) | SC-7(18) | SI-10 | SI-10(5) | SI-10(6) | SI-3(8)</td></tr>
</table>

Disrupt/Denial/Degrade
https://sparta.aerospace.org/technique/IMP-0002/
https://sparta.aerospace.org/technique/IMP-0003/
https://sparta.aerospace.org/technique/IMP-0004/

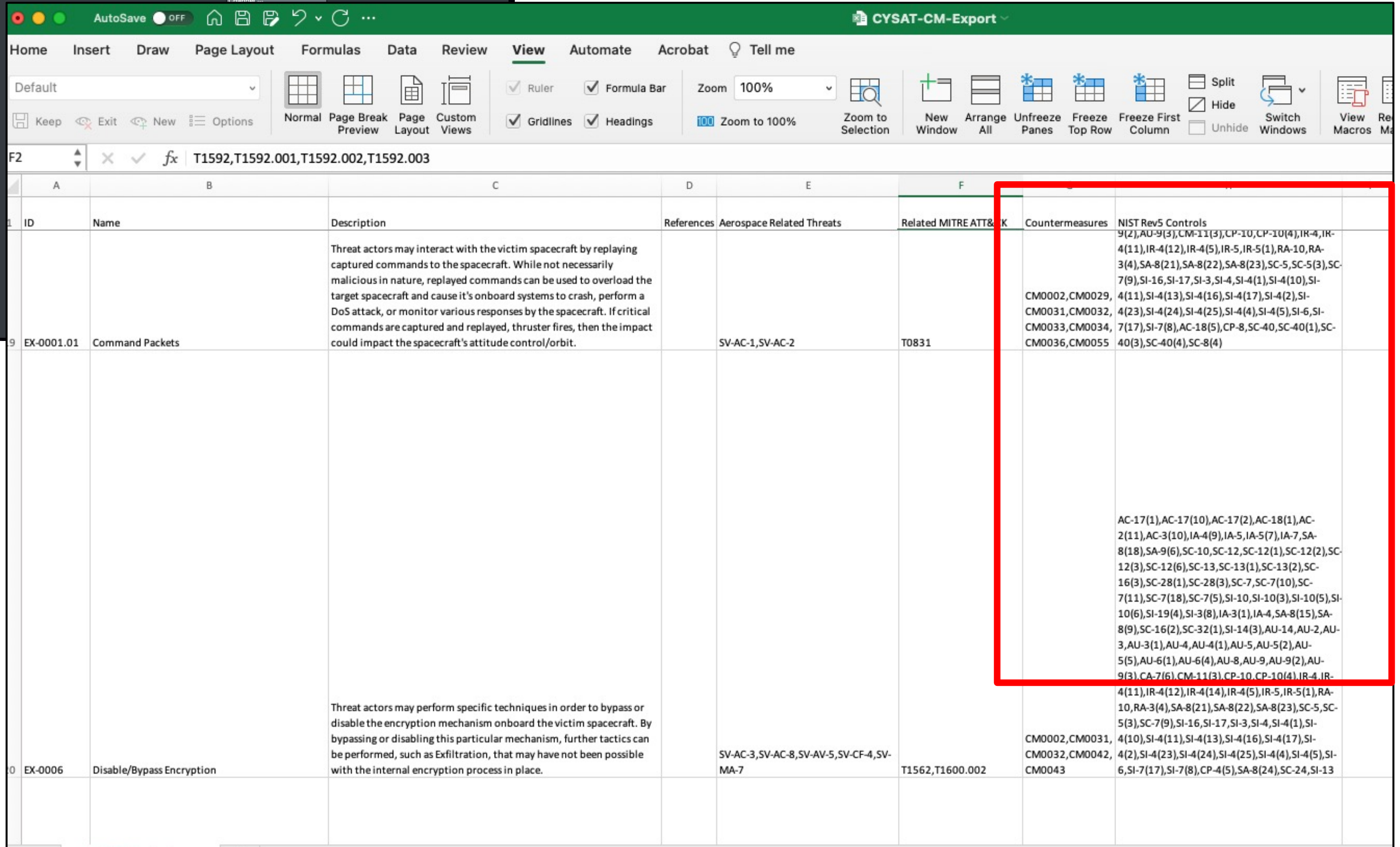
```
UG ] - GenericRWHardwareModel::uart_read_callback:  REQUEST C
UG ] - GenericRWHardwareModel::uart_read_callback:  REPLY   C
```

Combining the 4 Attack Chains

SPARTA Navigator – Extracting Countermeasures / NIST Controls



https://sparta.aerospace.org/navigator



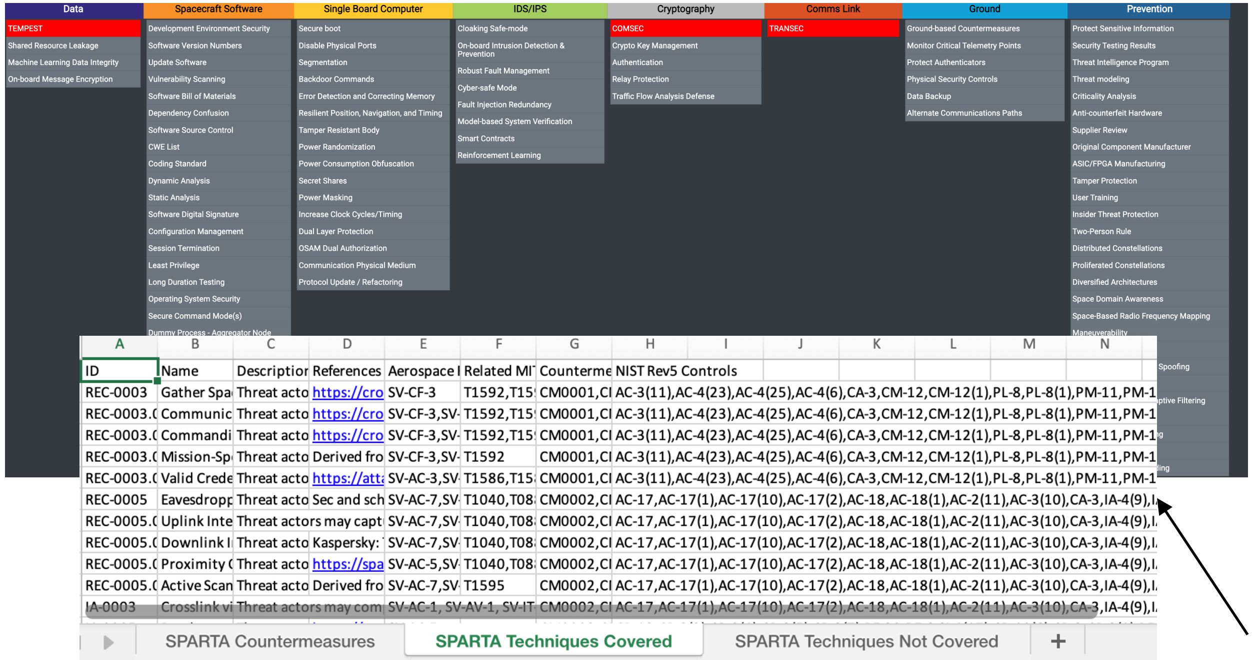
CM0001	CM0015	CM0028	CM0043
CM0002	CM0016	CM0029	CM0044
CM0003	CM0017	CM0030	CM0046
CM0004	CM0018	CM0031	CM0047
CM0005	CM0019	CM0032	CM0052
CM0007	CM0020	CM0033	CM0053
CM0008	CM0021	CM0034	CM0054
CM0009	CM0022	CM0035	CM0055
CM0010	CM0023	CM0036	CM0066
CM0011	CM0024	CM0038	CM0069
CM0012	CM0025	CM0039	CM0070
CM0013	CM0026	CM0040	CM0072
CM0014	CM0027	CM0042	CM0073

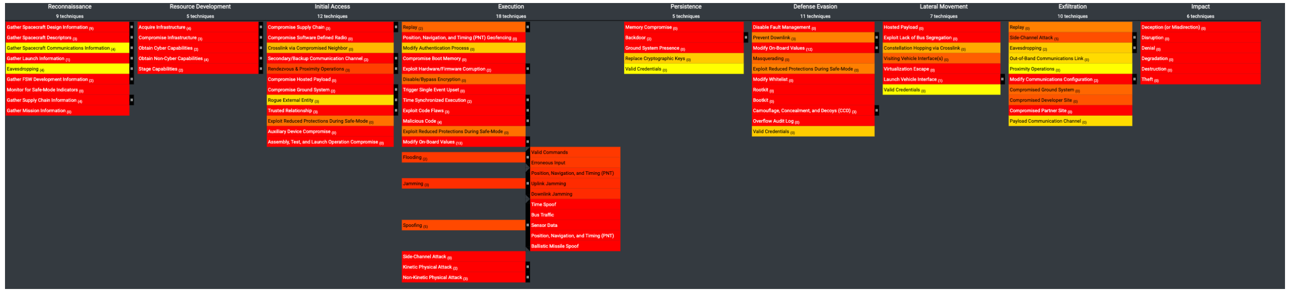
AC-3(11)	SA-10(7)	MA-3(1)	AC-3	SC-28(11)	CA-3(6)	SI-4(15)	CP-9	SI-10(5)
AC-4(23)	SA-11	MA-3(2)	AC-3(13)	SC-28(3)	CA-3(7)	SI-4(16)	CP-9(1)	SI-3(8)
AC-4(25)	SA-11(2)	MA-3(3)	AC-3(15)	SC-3	CA-7	SI-4(17)	CP-9(2)	PE-19
CM-12	SA-11(9)	MA-4	AC-3(4)	SC-38	CA-7(1)	SI-4(2)	CP-9(3)	PE-19(1)
CM-12(1)	SA-15	MA-4(1)	AC-4	SC-39	CA-7(6)	SI-4(20)	IA-11	PE-21
PM-11	SA-15(3)	MA-4(3)	AC-4(24)	SC-4	CA-8	SI-4(22)	IA-12	CP-11
PM-17	SA-15(7)	MA-4(6)	AC-4(26)	SC-45	CA-9	SI-4(23)	IA-12(1)	PM-16
SA-3(1)	SA-17	MA-4(7)	AC-4(31)	SC-45(1)	CM-10(1)	SI-4(24)	IA-12(2)	SA-15(8)
SA-3(2)	SA-2	MA-5(1)	AC-4(32)	SC-45(2)	CM-11	SI-4(25)	IA-12(3)	SC-32(1)
SA-4(12)	SA-22	MA-6	AC-6	SC-49	CM-11(2)	SI-4(4)	IA-12(4)	SA-10(3)
SA-5	SA-3	MA-7	AC-6(1)	SC-5	CM-11(3)	SI-4(5)	IA-12(5)	SA-10(4)
SA-9(7)	SA-4	MP-2	AC-6(10)	SC-5(1)	CM-14	SI-5	IA-12(6)	CA-8(3)
SI-21	SA-4(1)	MP-3	AC-6(2)	SC-5(2)	CM-2	SI-5(1)	IA-2	CM-4(1)
SI-23	SA-4(10)	MP-4	AC-6(3)	SC-5(3)	CM-2(2)	SI-6	IA-2(1)	SA-11(1)
SR-12	SA-4(2)	MP-5	AC-6(5)	SC-50	CM-2(3)	SI-7	IA-2(12)	SA-11(4)
SR-7	SA-4(3)	MP-5(4)	AC-6(8)	SC-51	CM-2(7)	SI-7(1)	IA-2(2)	SA-11(5)
AC-1	SA-4(5)	MP-6	AC-6(9)	SC-7	CM-3	SI-7(17)	IA-2(5)	SA-11(6)
AC-10	SA-4(7)	MP-6(3)	AC-7	SC-7(10)	CM-3(1)	SI-7(2)	IA-2(6)	SA-11(7)
AC-11	SA-4(9)	MP-7	AC-8	SC-7(11)	CM-3(2)	SI-7(5)	IA-2(8)	SA-11(8)
AC-11(1)	SA-8	PE-3(7)	AT-2(4)	SC-7(12)	CM-3(5)	SI-7(7)	IA-3	SA-15(5)
AC-12	SA-8(14)	PL-10	AT-2(5)	SC-7(13)	CM-3(7)	SI-7(8)	IA-3(1)	CM-7(4)
AC-12(1)	SA-8(15)	PL-11	AT-2(6)	SC-7(14)	CM-3(8)	SR-1	IA-4	RA-5(3)
AC-14	SA-8(18)	PL-8	AT-3	SC-7(18)	CM-4	SR-10	IA-4(9)	CM-8(7)
AC-16	SA-8(21)	PL-8(1)	AT-3(2)	SC-7(21)	CM-5(1)	SR-11	IA-5	SI-7(12)
AC-16(6)	SA-8(22)	PL-8(2)	AT-4	SC-7(25)	CM-5(5)	SR-11(1)	IA-5(1)	SI-7(15)
AC-17	SA-8(23)	PL-9	AU-10	SC-7(29)	CM-6	SR-11(2)	IA-5(13)	CM-5
AC-17(1)	SA-8(24)	PM-16(1)	AU-11	SC-7(3)	CM-6(1)	SR-11(3)	IA-5(14)	SI-7(9)

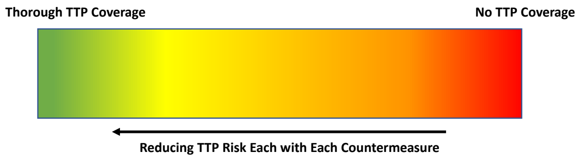
New SPARTA Countermeasure Mapper / Defensive Gap Analyzer

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

- Attack chains built in SPARTA's navigator can help identify countermeasures against the TTPs used in the attack
  - *Many users do not know TTPs, they only know the countermeasures they have implemented (or plan to)…*
- The SPARTA Gap Analyzer enables a graphical mechanism to select and deselect countermeasures from SPARTA's defense-in-depth view, *as the starting point*, to drive TTP mitigation & security planning
  - *It can export the data into Excel which provides tabs for coverage and gaps from a TTP perspective, including NIST controls*
- Below depicts the TTPs that have some mitigation when only applying COMSEC/TRANSEC/TEMPEST
  - ***Green/Yellow/Orange** indicates some level of coverage where **Red** indicates no coverage of the TTP*





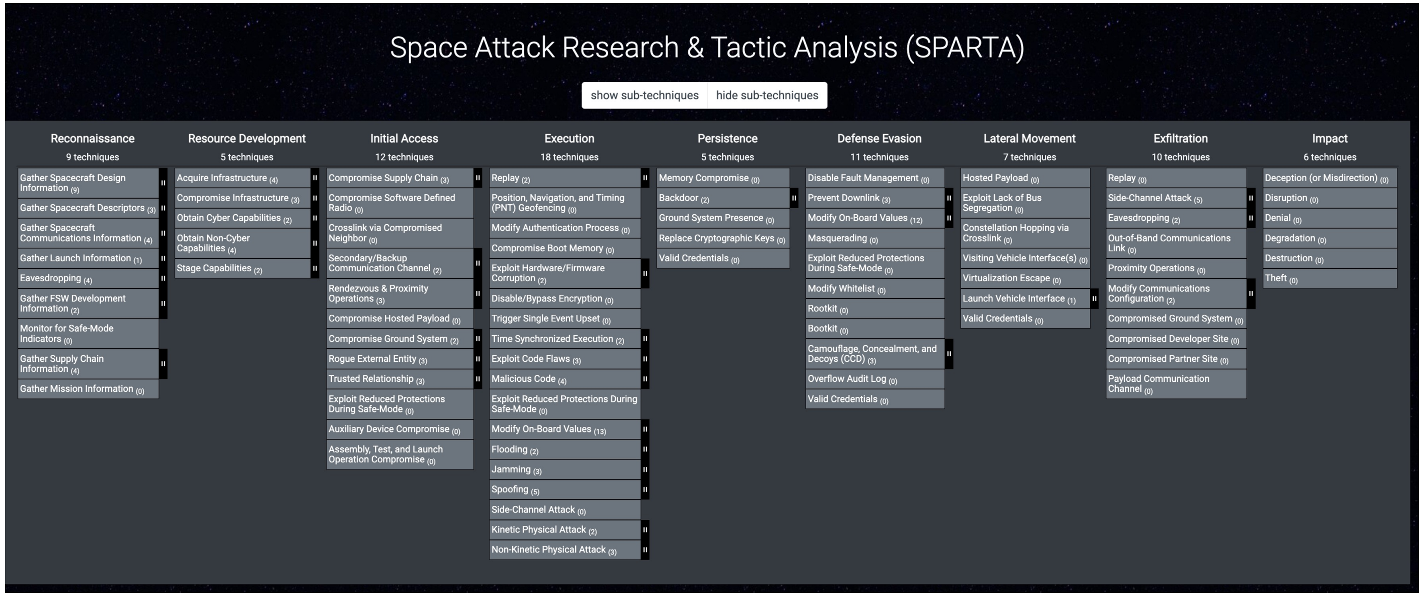


Excel Output

SPARTA

SPACE ATTACK RESEARCH & TACTIC ANALYSIS

https://sparta.aerospace.org



Sample Media Links:

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

Key SPARTA Links:

- Getting Started with SPARTA: https://sparta.aerospace.org/resources/getting-started | https://sparta.aerospace.org/resources/
- Understanding Space-Cyber TTPs with the SPARTA Matrix: https://aerospace.org/article/understanding-space-cyber-threats-sparta-matrix
- Leveraging the SPARTA Matrix: https://aerospace.org/article/leveraging-sparta-matrix
- Use Case w/ PCspooF: https://aerospacecorp.medium.com/sparta-cyber-security-for-space-missions-4876f789e41c & https://medium.com/the-aerospace-corporation/a-look-into-sparta-countermeasures-358e2fcd43ed
- FAQ: https://sparta.aerospace.org/resources/faq
- Matrix: https://sparta.aerospace.org
- Navigator: https://sparta.aerospace.org/navigator | Countermeasure Mapper: https://sparta.aerospace.org/countermeasures/mapper
- Related Work: https://sparta.aerospace.org/related-work/did-space with ties into TOR 2021-01333 REV A

Other Aerospace Papers and Resources

- DefCON Presentations:
  - DEF CON 2020: Exploiting Spacecraft
  - DEF CON 2021: Unboxing the Spacecraft Software BlackBox Hunting for Vulnerabilities
  - DEF CON 2022: Hunting for Spacecraft Zero Days using Digital Twins

- Papers/Articles:
  - 2019: Defending Spacecraft in the Cyber Domain
  - 2020: Establishing Space Cybersecurity Policy, Standards, & Risk Management Practices
  - 2021: Cybersecurity Protections for Spacecraft: A Threat Based Approach
  - 2021: The Value of Space
  - 2022: Protecting Space Systems from Cyber Attack

- July 2022 Congressional Testimony:
  - Video: https://science.house.gov/hearings?ID=996438A6-A93E-4469-8618-C1B59BC5A964
  - Written Testimony: https://republicans-science.house.gov/_cache/files/2/9/29fff6d3-0176-48bd-9c04-00390b826aed/A8F54300A11D55BEA5AF2CE305C015BA.2022-07-28-bailey-testimony.pdf

Theoretical Attack Chain - PCspooF

Example Attack Chains from the Past

2022 TTE Vulnerability - PCspooF

- Research paper by Andrew Loveless, Linh Thi Xuan Phan, Ronald Dreslinski and Baris Kasikci describing an attack dubbed PCspooF. The academic paper expertly articulates a [vulnerability in and exploit of Time-Triggered Ethernet (TTE)](), which is used as a bus service for a variety of spacecraft including NASA's Orion capsule, NASA's Lunar Gateway space station, and ESA's Ariane 6 launcher — among others.

PCspooF: Compromising the Safety of Time-Triggered Ethernet

Andrew Loveless*‡ Linh Thi Xuan Phan† Ronald Dreslinski* Baris Kasikci*
*University of Michigan †University of Pennsylvania ‡NASA Johnson Space Center
*{loveless, rdreslin, barisk}@umich.edu †linhphan@seas.upenn.edu

***Abstract*—Designers are increasingly using mixed-criticality networks in embedded systems to reduce size, weight, power, and cost. Perhaps the most successful of these technologies is Time-Triggered Ethernet (TTE), which lets critical time-triggered (TT) traffic and non-critical best-effort (BE) traffic share the same switches and cabling. A key aspect of TTE is that the TT part of the system is *isolated* from the BE part, and thus BE devices have no way to disrupt the operation of the TTE devices. This isolation allows designers to: (1) use untrusted, but low cost, BE hardware, (2) lower BE security requirements, and (3) ignore BE devices during safety reviews and certification procedures.**

We present PCspooF, the first attack to break TTE's isolation guarantees. PCspooF is based on two key observations. First, it is possible for a BE device to infer private information about the TT part of the network that can be used to craft malicious synchronization messages. Second, by injecting electrical noise into a TTE switch over an Ethernet cable, a BE device can trick the switch into sending these malicious synchronization messages to other TTE devices. Our evaluation shows that successful attacks are possible in seconds, and that each successful attack can cause TTE devices to lose synchronization for up to a second and drop tens of TT messages — both of which can result in the failure of critical systems like aircraft or automobiles. We also show that, in a simulated spaceflight mission, PCspooF causes uncontrolled maneuvers that threaten safety and mission success. We disclosed PCspooF to aerospace companies using TTE, and several are implementing mitigations from this paper.

***Index Terms*—Time-Triggered Ethernet, packet-in-packet attacks, electromagnetic interference, embedded systems**

I. Introduction

Increasingly, embedded systems are using *mixed-criticality* network technologies that allow traffic with different timing and fault tolerance requirements to coexist in the same physical network [1]–[4]. These technologies let designers reduce size, weight, power, and cost by sharing the same network between critical and non-critical parts of the system. For example, aircraft can share one network between vehicle control systems and passenger Wi-Fi and entertainment systems [5], [6]; spacecraft can share one network between life support systems and onboard experiments [7], [8]; and manufacturing plants can share one network between robot control systems and data collection systems [9].

One of the most successful mixed-criticality network technologies is *Time-Triggered Ethernet (TTE)* [2], Today, TTE serves as the network backbone for several spacecraft, including NASA's Orion capsule [10], NASA's Lunar Gateway space station [7], and ESA's Ariane 6 launcher [11]. TTE is also widely used in aircraft [12]–[14], energy generation systems [15], and industrial control systems [16], [17], and is a leading contender to replace CAN bus and FlexRay as the standard network technology in future automobiles [18], [19].

TTE has several properties that make it attractive for safety and mission-critical applications. Most notably, TTE follows a *time-triggered (TT)* paradigm, in which devices are tightly synchronized, and they send messages and execute software according to a predetermined schedule. This TT approach reduces message latencies to hundreds of microseconds and jitter to near-zero [20], [21], making TTE appropriate for even the tightest control loops. TTE also provides fault tolerance by replicating the whole network to form multiple *planes*, and by forwarding messages over all planes simultaneously [22].

In addition, TTE enables mixed-criticality architectures by being 100% compatible with standard Ethernet [23]. This means that *non-critical* systems, which typically use standard Ethernet hardware to lower costs [24], can send messages over the same cabling as the critical TTE devices. Unlike TT traffic, standard Ethernet traffic is forwarded on a *best-effort (BE)* basis, filling in space *around* the TT traffic [23]. Also, standard Ethernet traffic typically only travels over a single network plane, so does not have any fault tolerance guarantees [7].

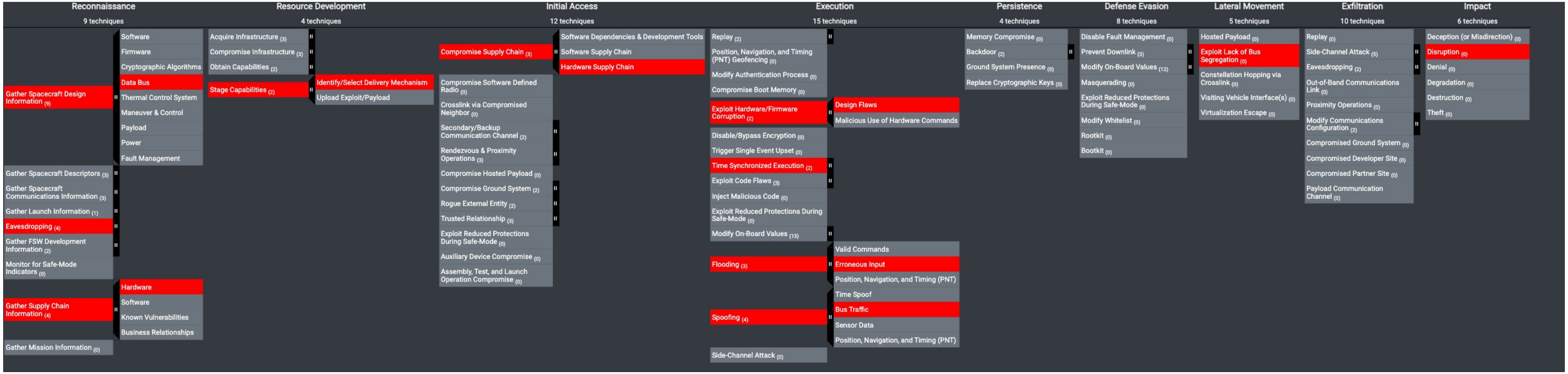
A key aspect of TTE's mixed-criticality design is that the TT part of the system is *isolated* from the BE part. In other words, no matter how the BE devices behave, they should not be able to disrupt synchronization between TTE devices, or the timely or successful delivery of TT traffic [25]. This isolation is commonly used as justification for several cost-cutting measures, including: (1) procuring BE devices from relatively untrusted (but low cost) suppliers [26], [27]; (2) relaxing security requirements for BE devices [28]; and (3) reducing the scope of analysis and certification of a system to focus solely on the TTE devices [29]. For example, on NASA spacecraft, onboard experiments are often provided by university research groups, are operated by the university students with minimal NASA involvement, and are not considered in safety reviews or the certification process of the overall vehicle [30], [31].

In this paper, we present PCspooF, a new attack that breaks TTE's isolation guarantees for the first time — allowing a single malicious BE device on a single plane to disrupt synchronization and communication between TTE devices on all planes. PCspooF is based on two key observations:

First, it is possible for a malicious BE device to *infer* private information about the TTE network that is needed to construct valid TTE synchronization messages, called *protocol control*

Example Attack Chains from the Past

PCspooF Potential Attack Chain



Introducing SPARTA using PCSpooF: Cyber Security for Space Missions - https://medium.com/the-aerospace-corporation/sparta-cyber-security-for-space-missions-4876f789e41c
A Look into SPARTA Countermeasures - https://medium.com/the-aerospace-corporation/a-look-into-sparta-countermeasures-358e2fcd43ed

PCspooF Countermeasure Samples

Quick Way to Identify Potential Mitigations

Introducing SPARTA using PCSpooF: Cyber Security for Space Missions - https://medium.com/the-aerospace-corporation/sparta-cyber-security-for-space-missions-4876f789e41c

A Look into SPARTA Countermeasures - https://medium.com/the-aerospace-corporation/a-look-into-sparta-countermeasures-358e2fcd43ed

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 c

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 Co
- 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.

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

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-persistence | 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 deni
.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
to deploy malware to latera
has the ability to connect vi
pecific command set. The co
y to command hosted payloa