Best Practice Guideline for Logging Events of Space Vehicle Sub-Systems

Submitted by:
Stephenson Stellar Corporation
Intertech Park Box 5
2031 Kings Highway
Shreveport, LA 71103
Questions/Comments: SV-Logging-BPG@stephensonstellar.org

CAGE Code: 88AS9
Unique Entity Identifier: NV8KK5L2AF44

Date of Submittal: August 7, 2024

REVISION HISTORY

Revision Number	Revision Date	Nature of Revision
Distro_A-v1	08/07/2024	Delivery of initial document set for Public Release.

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

Effective logging within the subsystems of a Space Vehicle (SV) will enable operators to quickly diagnose and troubleshoot issues and enhance the space system's overall security posture. At the time of this research, there have been no guidelines instituted to provide insight into what should be logged within the individual subsystems of an SV that would highlight indicators of malicious cyber activity.

These guidelines have been captured and organized into a spreadsheet that is intended to be a guideline as to what should be evaluated and logged within each spacecraft subsystem. This guideline of best practices was derived from analysis of the Aerospace Corporation's Space Attack Research and Tactic Analysis (SPARTA) framework and through specialized research performed by Stephenson Stellar Corporation (SSC) using their Stellar Space & Cyber Range (SSCR) located in Colorado Springs, Colorado.

Each SV will have a unique design and differing capabilities/payloads, so this guideline is intended to be a starting point of logging best practices that can be applied to enhance the SV security posture. This is not intended to be a requirements document. However, these guidelines can be applied where applicable and used to assist space organizations with defining their overall computer network defense strategy and cyber protections of operational spacecraft.

1. INTRODUCTION AND APPROACH

1.1 Introduction

Until recently, most space-based systems were developed under the auspice that space was "untouchable." Once a vehicle was launched, it was considered out of reach of our adversaries, and—if encrypted links were utilized—the mission and data were considered safe. This is no longer the case. During the conflict between Russia and Ukraine, Russian hackers targeted a United States-based satellite company (ViaSat) to disrupt communications in one of the most significant cyberattacks to date on space systems. Even as early as 2008, satellite hijacking was demonstrated by hackers gaining access to the Landsat-7 satellite, achieving all steps required for remote commanding of the vehicle. With space becoming an increasingly contested environment, and advancements of technology bringing Internet Protocol (IP) to mesh architectures in space, the ability to record events that occur within the spacecraft itself should be the heart of the SV security strategy. The best way to ensure those events are tracked and stored is to implement a comprehensive security log management framework.

Log files are detailed, text-based records of events within an organization's Information Technology (IT) and Operational Technology (OT) systems. Within the space enterprise, logs can be generated by a wide variety of devices and applications. Some examples of these are anti-malware, system utilities, firewalls, Intrusion Detection Systems (IDS)/Intrusion Prevention Systems (IDSs/IPSs), servers, workstations, networking equipment, and Fault Management Systems (FMS). This best practice guide for logging events within SV subsystems can provide a vitally important audit trail and can be used to monitor activity within the SV infrastructure. These logs will enable the monitoring teams to identify policy violations, pinpoint fraudulent or unusual activity and highlight security incidents or anomalies that occur within the spacecraft.

The vision is that security teams will be able to use these logs from the spacecraft subsystems to detect and respond to anomalies or indicators of compromise, investigate, and analyze where activity is coming or came from, and determine if the activity will have an impact on the mission of the SV or potentially have cascading affects to other subsystems or other SVs within the constellation. Additionally, these logs can hopefully be correlated with the logs collected from other segments of the space enterprise including the ground and link components.

1.2 Approach

The approach was to analyze existing bodies of work and use research being performed by SSCR to identify known and possible attack vectors targeting the individual subsystems of the SV. The main sources used to identify these potential vectors were the Aerospace Corporation's SPARTA framework and other potential vectors discovered through research within the SSCR.

1.2.1 Aerospace SPARTA Framework

Aerospace Corporation created the SPARTA matrix to address the information and communication barriers that hinder the identification and sharing of space-system Tactics, Techniques, and Procedures (TTPs). SPARTA is intended to provide unclassified information to space professionals about how spacecraft may be compromised via cyber and traditional

counterspace means. The matrix defines and categorizes commonly identified activities that could contribute to spacecraft compromises.

SPARTA is beneficial when evaluating the vulnerabilities and determining pathways and TTPs an unauthorized user may use on the Space Segment assets.

Figure 1 below is a depiction of SPARTA showing the different phases of attack and the techniques that are used within each of the phases. For more details on SPARTA, go to SPARTA (https:/sparta.aerospace.org).

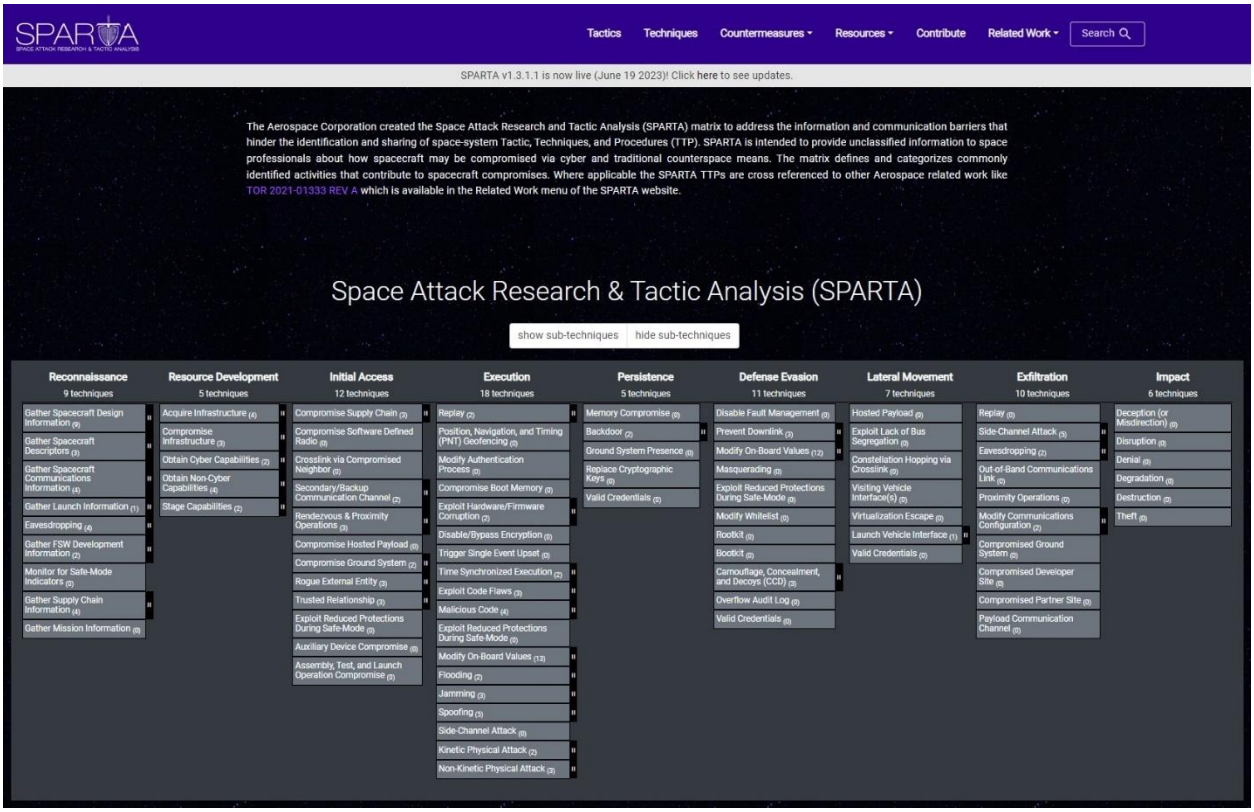


Figure 1. SPARTA Main Page

0 contains an embedded spreadsheet - the Space Vehicle Logging Best Practice Guide matrix. Within the matrix is a deconstruction of SPARTA with applied analytics using the SSCR to identify which subsystems these attack vectors could be applied to.

1.2.2 SSCR

SSCR is a space focused cyber range funded through the Air Force Research Laboratory (AFRL) Information Directorate for the purpose of supporting the Space Force and other organizations through the research, experimentation, training, and whole-of-government education in the space and cyberspace domains. SSCR has been designed, constructed, and operated by SSC, a 501(c)(3) nonprofit research and development company that specializes in space-based cybersecurity. This space cyber range can also be leveraged as a platform for Research, Development, Test, and

Evaluation (RDT&E) of TTPs and as a hands-on training tool to accompany SSC's workshop delivery of space and cybersecurity operational concepts.

SSCR consists of multiple representative space systems that serve as an initial capability and precursor to an unfunded on-orbit cyber range called the Cybersecurity Pathfinder Constellation (CPC), a space-based testbed constellation consisting of four Low Earth Orbit (LEO) satellites that would offer protected experimentation and on-orbit cyber exploitation. As shown in Figure 2, the range was designed to offer a simulated satellite system that replicates the CPC.

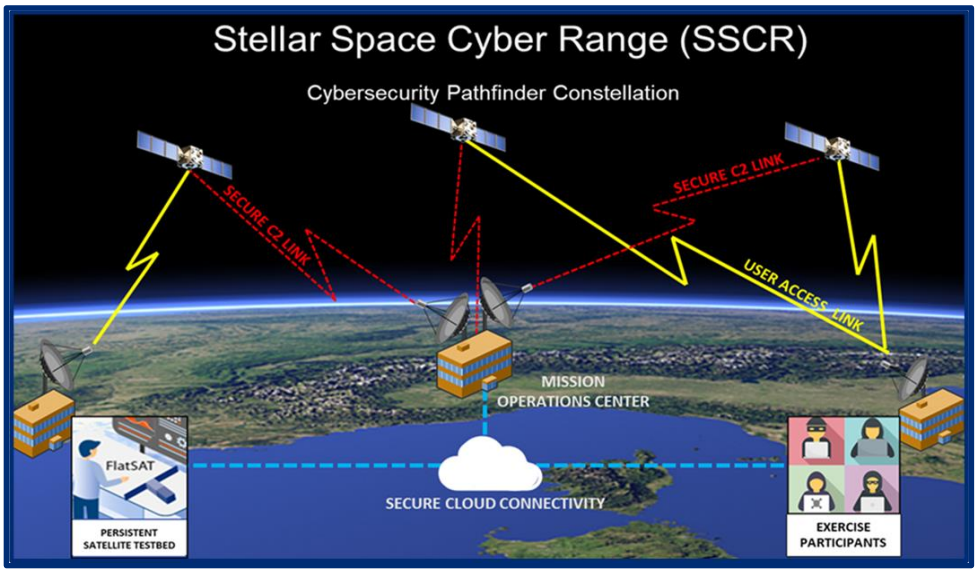


Figure 2. SSCR Pathfinder Constellation and Cyber Range Operational Overview

To support this specialized research, the lab consists of three FlatSats, physics simulation software, embedded flight computer software, and host Personal Computers (PCs) that mimic the capabilities of a ground station (i.e., planning, scheduling, tasking, command, and control).

Many of the logging recommendations were derived from research associated with the SSCR for Zero Trust Architectures (ZTA) for Space Systems and through live activities and hosted workshops. The logging recommendations are based off likely attack vectors that have been identified through these events and research efforts.

2. BEST PRACTICE GUIDELINES FOR LOGGING EVENTS

2.1 SV Subsystems Overview

The data entry point to a spacecraft is the antenna and the Radio Frequency (RF) front-end transceiver. The antenna is the most important component of the communications subsystem, as this is where the electromagnetic signals are originated and received. Once those signals are received, they are de-modulated and transmitted to one of the various spacecraft sub-systems:

- **Command & Data Handling (C&DH) Subsystem**—The main computing and data flow controller in the satellite, also referred to as the On-Board Computer (OBC). In addition to the main microprocessor, this may contain analog-to-digital converters, an internal communications bus or buses, mass memory storage, and attitude control processing.
- **Attitude Determination and Control Subsystem (ADCS)**—The sensors, actuators, and sometimes computing power used to control the orientation of the spacecraft relative to some reference coordinate system. This is sometimes grouped with the orbital position determination subsystem.
- **Guidance, Navigation, and Control (GN&C) Subsystem**—Sometimes referred to as the Orbit Determination and Control (ODC) subsystem, this may overlap with the ADCS. It contains all the sensors and computation necessary to determine and control the spacecraft orbit, including rendezvous and proximity operations. In earth orbit, it often includes a Global Positioning System (GPS) receiver.
- **Electrical Power Subsystem (EPS)**—The power collection or production, storage, distribution, and management subsystem.
- **Telemetry, Tracking, and Communications (TT&C) Subsystem**—The radios and modems, antenna(s), cabling, and any other components used to communicate with the ground or other spacecraft. This also may be referred to as just the Communications Subsystem (Comm).
- **Propulsion (Prop) Subsystem**—The nozzles and thrusters, fuel tanks, piping, valves, and other components used to provide thrust for altering a spacecraft's trajectory and sometimes controlling attitude.
- **Thermal Control Subsystem (TCS)**—All the hardware necessary to control the temperature of spacecraft components within their safety and operational limits. This always includes passive components such as radiators and blankets, and also may include active components such as heaters and coolers.
- **Structures and Mechanisms Subsystem (SMS)**—The supporting framework of the spacecraft which must be designed to withstand launch vibrations and loads. This is sometimes referred to as the mechanical bus. It may include moving mechanisms such as antenna gimbals and protective doors.
- **Payload or Instrument**—All other subsystems exist for the benefit of the payload(s). It fulfills the mission(s) of the spacecraft, whether it be data collection, signals and communications relay, or other.

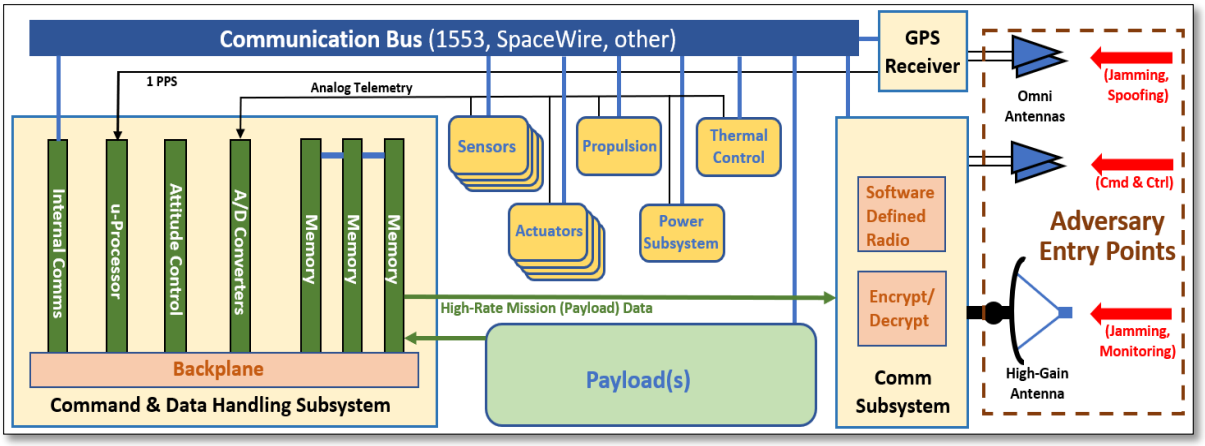


Figure 3. On-Board Spacecraft Communications

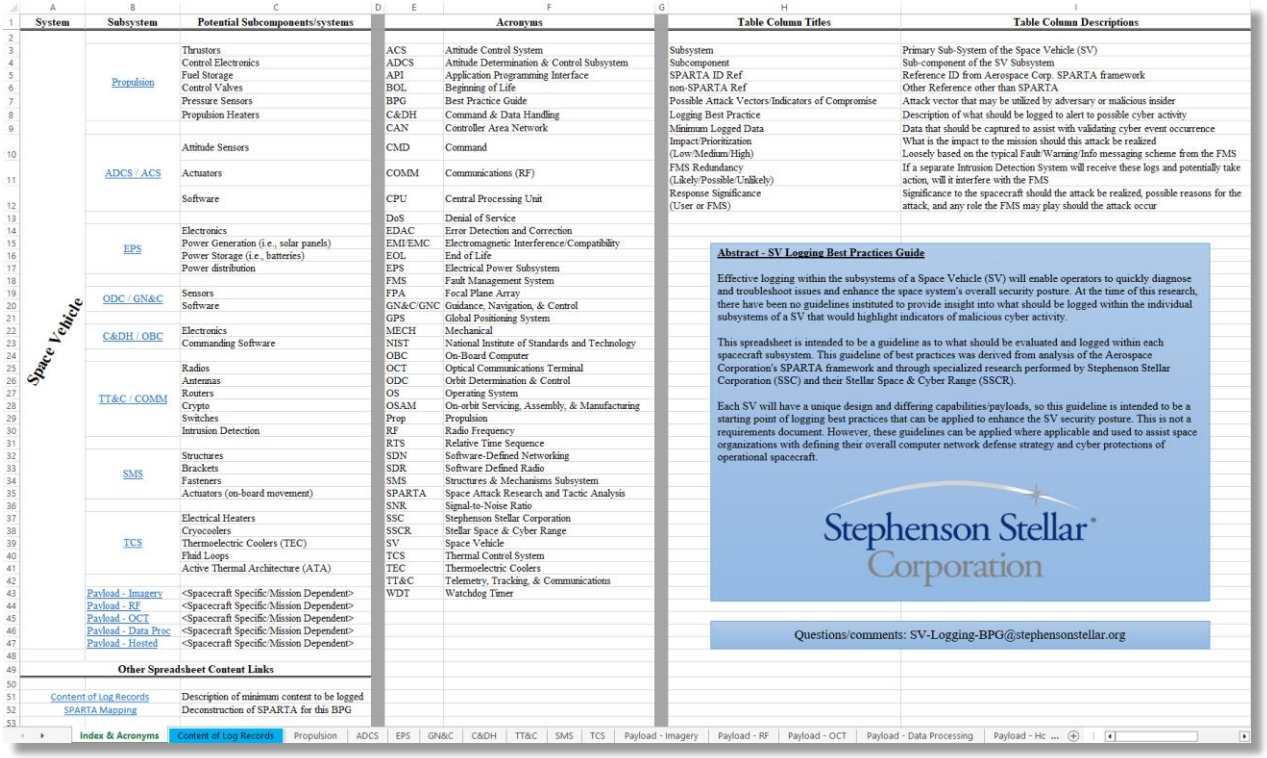
There are times when the ground system communicates directly with a subsystem or when subsystems communicate with each other on the SV. As depicted in Figure 3, all communications need to be monitored and capable of logging and alerting when behavior is off nominal.

2.2 Logging Best Practices for SV Spreadsheet Overview

The spreadsheet that is included as 0 was constructed to be used as a guideline for logging event types for each of the primary SV subsystems. This section will give an overview of the spreadsheet construct and what is contained within the various tabs.

2.2.1 Index

The first tab of the spreadsheet (Figure 4) contains the index. This index contains a listing of the SV subsystems, the subcomponents of the subsystem, acronyms used throughout the spreadsheet, a listing of the column headers, and descriptions of what is in each column. Additionally, there is an abstract of the spreadsheet describing the purpose and the contents within. The user can navigate to each subsystem by either clicking on the link provided in the subsystem column, or by selecting the tab at the bottom of the spreadsheet.



System	Subsystem	Potential Subcomponents/systems
Space Vehicle	Propulsion	Thrustors
		Control Electronics
		Fuel Storage
		Control Valves
		Pressure Sensors
		Propulsion Heaters
	ADCS / ACS	Attitude Sensors
		Actuators
		Software
	EPS	Electronics
		Power Generation (i.e., solar panels)
		Power Storage (i.e., batteries)
		Power distribution
	ODC / GN&C	Sensors
		Software
	C&DH / OBC	Electronics
		Commanding Software
	TT&C / COMM	Radios
		Antennas
		Routers
		Crypto
		Switches
		Intrusion Detection
	SMS	Structures
		Brackets
		Fasteners
		Actuators (on-board movement)
	TCS	Electrical Heaters
		Cryocoolers
		Thermoelectric Coolers (TEC)
		Fluid Loops
		Active Thermal Architecture (ATA)
	Payload - Imagery	<Spacecraft Specific/Mission Dependent>
	Payload - RF	<Spacecraft Specific/Mission Dependent>
	Payload - OCT	<Spacecraft Specific/Mission Dependent>
	Payload - Data Proc	<Spacecraft Specific/Mission Dependent>
	Payload - Hosted	<Spacecraft Specific/Mission Dependent>

Other Spreadsheet Content Links	
Content of Log Records	Description of minimum content to be logged
SPARTA Mapping	Deconstruction of SPARTA for this BPG

Acronyms	
ACS	Attitude Control System
ADCS	Attitude Determination & Control Subsystem
API	Application Programming Interface
BOL	Beginning of Life
BPG	Best Practice Guide
C&DH	Command & Data Handling
CAN	Controller Area Network
CMD	Command
COMM	Communications (RF)
CPU	Central Processing Unit
DoS	Denial of Service
EDAC	Error Detection and Correction
EMI/EMC	Electromagnetic Interference/Compatibility
EOL	End of Life
EPS	Electrical Power Subsystem
FMS	Fault Management System
FPA	Focal Plane Array
GN&C/GNC	Guidance, Navigation, & Control
GPS	Global Positioning System
MECH	Mechanical
NIST	National Institute of Standards and Technology
OBC	On-Board Computer
OCT	Optical Communications Terminal
ODC	Orbit Determination & Control
OS	Operating System
OSAM	On-orbit Servicing, Assembly, & Manufacturing
Prop	Propulsion
RF	Radio Frequency
RTS	Relative Time Sequence
SDN	Software-Defined Networking
SDR	Software Defined Radio
SMS	Structures & Mechanisms Subsystem
SPARTA	Space Attack Research and Tactic Analysis
SNR	Signal-to-Noise Ratio
SSC	Stephenson Stellar Corporation
SSCR	Stellar Space & Cyber Range
SV	Space Vehicle
TCS	Thermal Control System
TEC	Thermoelectric Coolers
TT&C	Telemetry, Tracking, & Communications
WDT	Watchdog Timer

Table Column Titles	Table Column Descriptions
Subsystem	Primary Sub-System of the Space Vehicle (SV)
Subcomponent	Sub-component of the SV Subsystem
SPARTA ID Ref	Reference ID from Aerospace Corp. SPARTA framework
non-SPARTA Ref	Other Reference other than SPARTA
Possible Attack Vectors/Indicators of Compromise	Attack vector that may be utilized by adversary or malicious insider
Logging Best Practice	Description of what should be logged to alert to possible cyber activity
Minimum Logged Data	Data that should be captured to assist with validating cyber event occurrence
Impact/Prioritization (Low/Medium/High)	What is the impact to the mission should this attack be realized
FMS Redundancy (Likely/Possible/Unlikely)	Loosely based on the typical Fault/Warning/Info messaging scheme from the FMS
Response Significance (User or FMS)	If a separate Intrusion Detection System will receive these logs and potentially take action, will it interfere with the FMS
	Significance to the spacecraft should the attack be realized, possible reasons for the attack, and any role the FMS may play should the attack occur

Abstract - SV Logging Best Practices Guide

Effective logging within the subsystems of a Space Vehicle (SV) will enable operators to quickly diagnose and troubleshoot issues and enhance the space system's overall security posture. At the time of this research, there have been no guidelines instituted to provide insight into what should be logged within the individual subsystems of a SV that would highlight indicators of malicious cyber activity.

This spreadsheet is intended to be a guideline as to what should be evaluated and logged within each spacecraft subsystem. This guideline of best practices was derived from analysis of the Aerospace Corporation's SPARTA framework and through specialized research performed by Stephenson Stellar Corporation (SSC) and their Stellar Space & Cyber Range (SSCR).

Each SV will have a unique design and differing capabilities/payloads, so this guideline is intended to be a starting point of logging best practices that can be applied to enhance the SV security posture. This is not a requirements document. However, these guidelines can be applied where applicable and used to assist space organizations with defining their overall computer network defense strategy and cyber protections of operational spacecraft.

Stephenson Stellar Corporation

Questions/comments: SV-Logging-BPG@stephensonstellar.org

Index & Acronyms | Content of Log Records | Propulsion | ADCS | EPS | GN&C | C&DH | TT&C | SMS | TCS | Payload - Imagery | Payload - RF | Payload - OCT | Payload - Data Processing | Payload - Hc ...

Figure 4. Index Tab

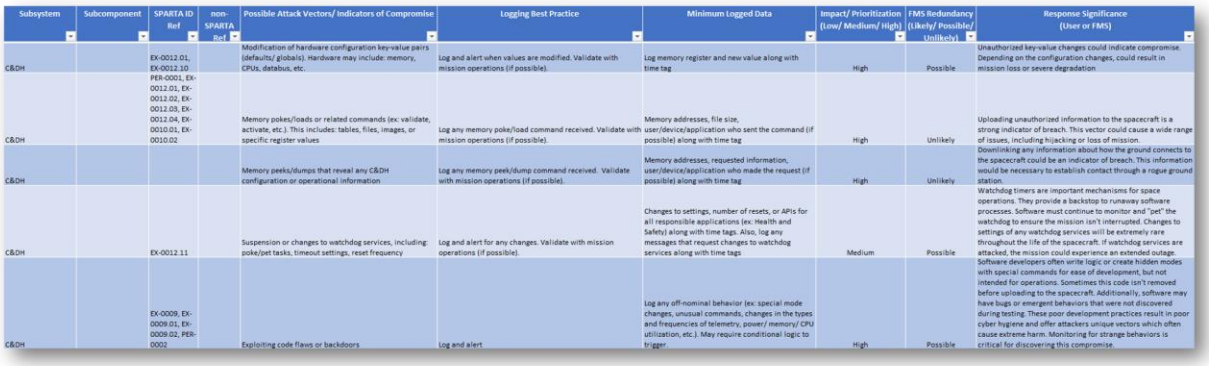
2.2.2 Content of Log Records Tab

System logs serve as a vital tool for auditing and forensic analysis, helping organizations detect and investigate suspicious activities. To ensure effective auditing, system logs must capture a comprehensive set of data points.

Understanding the baseline or minimum content that should be recorded in these logs is essential for maintaining security, ensuring compliance, and mitigating risks. The purpose of the "Content of Log Record" tab is to list and describe the minimum content that should be recorded in logs according to the NIST 800-53 v5, AU-3 and AU-3 (1) security controls. This includes detailed event descriptions, precise timestamps, and both source and destination addresses. Additionally, logs should record user or process identifiers, success or failure indications, and any filenames associated with the event. By capturing these elements, organizations can accurately trace the sequence of actions and identify anomalies or unauthorized activities within their systems.

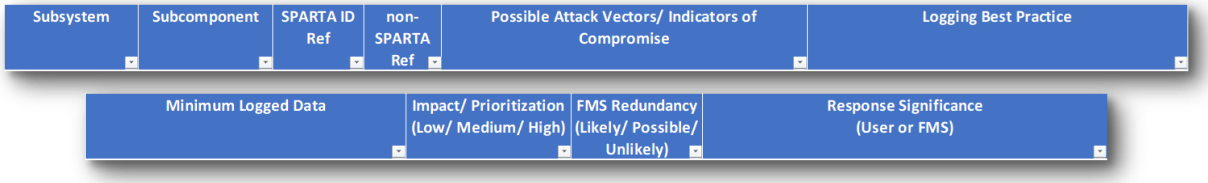
2.2.3 Subsystem Tabs and Column Descriptions

When a user clicks on the Subsystem links or selects a Subsystem tab, they will be directed to a workbook for a particular subsystem. A portion of the C&DH tab is shown below (Figure 5) as an example.



Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/ Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/ Prioritization (Low/ Medium/ High)	FMS Redundancy (Likely/ Possible/ Unlikely)	Response Significance (User or FMS)
C&DH		EX-0012.01, EX-0012.10		Modification of hardware configuration key-value pairs (defaults/ globals). Hardware may include: memory, CPUs, databus, etc.	Log and alert when values are modified. Validate with mission operations (if possible).	Log memory register and new value along with time tag	High	Possible	Unauthorized key-value changes could indicate compromise. Depending on the configuration changes, could result in mission loss or severe degradation
C&DH		PER-0001, EX-0012.01, EX-0012.02, EX-0012.03, EX-0012.04, EX-0010.01, EX-0010.02		Memory pokes/loads or related commands (ex: validate, activate, etc.). This includes: tables, files, images, or specific register values	Log any memory poke/load command received. Validate with mission operations (if possible).	Memory addresses, file size, user/device/application who sent the command (if possible) along with time tag	High	Unlikely	Uploading unauthorized information to the spacecraft is a strong indicator of breach. This vector could cause a wide range of issues, including hijacking or loss of mission.
C&DH				Memory peeks/dumps that reveal any C&DH configuration or operational information	Log any memory peek/dump command received. Validate with mission operations (if possible).	Memory addresses, requested information, user/device/application who made the request (if possible) along with time tag	High	Unlikely	Downlinking any information about how the ground connects to the spacecraft could be an indicator of breach. This information would be necessary to establish contact through a rogue ground station.
C&DH		EX-0012.11		Suspension or changes to watchdog services, including: poke/pet tasks, timeout settings, reset frequency	Log and alert for any changes. Validate with mission operations (if possible).	Changes to settings, number of resets, or APIs for all responsible applications (ex: Health and Safety) along with time tags. Also, log any messages that request changes to watchdog services along with time tags	Medium	Possible	Watchdog timers are important mechanisms for space operations. They provide a backstop to runaway software processes. Software must continue to monitor and "pet" the watchdog to ensure the mission isn't interrupted. Changes to settings of any watchdog services will be extremely rare throughout the life of the spacecraft. If watchdog services are attacked, the mission could experience an extended outage.
C&DH		EX-0009, EX-0009.01, EX-0009.02, PER-0002		Exploiting code flaws or backdoors	Log and alert	Log any off-nominal behavior (ex: special mode changes, unusual commands, changes in the types and frequencies of telemetry, power/ memory/ CPU utilization, etc.). May require conditional logic to trigger.	High	Possible	Software developers often write logic or create hidden modes with special commands for ease of development, but not intended for operations. Sometimes this code isn't removed before uploading to the spacecraft. Additionally, software may have bugs or emergent behaviors that were not discovered during testing. These poor development practices result in poor cyber hygiene and offer attackers unique vectors which often cause extreme harm. Monitoring for strange behaviors is critical for discovering this compromise.

Figure 5. C&DH Subsystem Tab



Subsystem	Subcomponent	SPARTA ID Ref	non-SPARTA Ref	Possible Attack Vectors/ Indicators of Compromise	Logging Best Practice	Minimum Logged Data	Impact/ Prioritization (Low/ Medium/ High)	FMS Redundancy (Likely/ Possible/ Unlikely)	Response Significance (User or FMS)

Figure 6. Column Headers within each Subsystem Tab

Below are the descriptions of the columns (see Figure 6) depicted in each subsystem tab.

- **Subsystem**: Each space vehicle has a set of subsystems that contribute to the overall functionality of the space vehicle such as propulsion, navigation, communication, power generation, payload, etc. The subsystems are tabbed at the bottom of the excel sheet.
- **Subcomponent**: Each subsystem has subcomponents within that have defined roles. For example, within the communication subsystem, the radios, antennas, routers, and encryptors are some of the subcomponents. These subcomponents are crucial to log and monitor for any type of anomalies or issues that may arise.
- **SPARTA ID Ref**: This is the Reference ID from the Aerospace Corporation's SPARTA framework. These are used to reference specific parts of the framework in the context of logging best practices.
- **Non-SPARTA Ref**: Any reference that does not originate from the SPARTA framework.
- **Possible Attack Vectors/Indicators of Compromise**: These are potential attack methods an adversary could use to compromise a spacecraft system or signs a compromise has occurred.
- **Logging Best Practice**: This is the recommendation of what should be logged to alert on possible compromises or provide sufficient detail for troubleshooting and network forensics.

- **Minimum Logged Data**: This is the bare essential data that should be captured in logs to assist with troubleshooting or cyber network forensics. An example of this is timestamps, memory register values, file sizes, or error messages.
- **Impact/Prioritization**: This refers to assessing the impact to a mission if an attack is carried out and successful. This is loosely based on the Fault, Warning, Info messaging scheme from the FMS and is given a Low, Medium, or High assessment.
- **Fault Management Redundancy**: This describes what happens if a separate IDS will receive these logs and potentially take action and/or will it interfere with the FMS. This is given a Likely, Possible, or Unlikely assessment.
- **Response Significance**: Significance to the spacecraft should the attack be realized, possible reasons for the attack, and any role the FMS may play should the attack occur.

2.2.4 SPARTA Mapping Tabs

The SPARTA Mapping tab contains a table that lists all attacks (extracted from SPARTA) that are directed specifically at the spacecraft's subsystems. Each of these attacks is separately identified via their SPARTA ID reference number, which can also be cross-referenced on the remaining Subsystem Tabs of the spreadsheet in 0. Each attack has an included description directly from SPARTA and is further broken down into the affected Subsystem, Sub-component, Data Type, and associated Attack Vector. This information is used to categorize and breakdown each attack to properly generate recommendations for logging best practices.

3. CONCLUSIONS

The spacecraft itself has been a blind spot when it comes to cybersecurity. With the rapid increase in technology and IT enhancements within the space enterprise, there is also a rapid increase in the amount of attack vectors available to our adversaries. Establishing a capability to log events and anomalous behavior on spacecraft and enable log integration and correlation with the rest of the enterprise will greatly enhance cyber situational awareness in the space domain.

This best practice guideline has been derived as a first step in logging events within the spacecraft subsystems. The guide does not cover storage practices, protection of the log files, retention/deletion, or the process for integrating these logs into an enterprise Security Information and Event Management (SIEM) solution. This guide was designed to help space developers and customers determine what events to log and types of data to capture during the logging.

It will be essential that the cyber teams, Security Operations Centers, and SV operators define and implement an efficient management and analysis process of the logs. This includes integration into an enterprise SIEM, logging policies for SVs, log management, and further into the future autonomous response.

APPENDIX A: SPACE VEHICLE LOGGING BEST PRACTICE GUIDE

Embedded spreadsheet:

Space_Vehicle_Loggin
g_Best_Practices-Distr

APPENDIX B: REFERENCES

Application of Zero Trust Architecture to Spacecraft—Stephenson Stellar.pdf. (n.d.).

Cyber Threats to Space Systems. (n.d.). Joint Air Power Competence Centre. Retrieved February 4, 2021, from https://www.japcc.org/cyber-threats-to-space-systems/

Cyberwarfare in space: Satellites at risk of hacker attacks. (n.d.). ZDNET. Retrieved November 3, 2023, from https://www.zdnet.com/article/cyberwarfare-in-space-satellites-at-risk-of-hacker-attacks/

MITRE ATT&CK®. (n.d.). Retrieved November 3, 2023, from https://attack.mitre.org/

Aerospace SPARTA. (n.d.). Retrieved November 3, 2023, from https://sparta.aerospace.org/

Poireault, K. (2023, May 9). *Five Takeaways From the Russian Cyber-Attack on Viasat's Satellites*. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/takeaways-russian-cyberattack/

Turla APT Group Abusing Satellite Internet Links. (2015, September 9). https://threatpost.com/turla-apt-group-abusing-satellite-internet-links/114586/

ZERO-TRUST FOR ZERO-GRAVITY. (2023, September 29). *Spideroak*. https://spideroak.com/zero-trust-for-zero-gravity/

APPENDIX C: ACRONYMS

Acronym	Definition	Context
ADCS	Attitude Determination and Control Subsystem	The Sensors, actuators, and sometimes computing power used to control the orientation of the spacecraft relative to some reference coordinate system. This is sometimes grouped with the orbital position determination subsystem.
AFRL	Air Force Research Laboratory	Leads the discovery, development, and delivery of warfighting technologies for United States air, space, and cyberspace forces.
ATT&CK	Adversarial Tactics, Techniques, and Common Knowledge	A knowledge base of adversary tactics and techniques based on real-world observations.
C&DH	Command & Data Handling	The main computing and data flow controller in the satellite, also referred to as the On-Board Computer (OBC). In addition to the main microprocessor, this may contain analog-to-digital converters, an internal communications bus or buses, mass memory storage, and attitude control processing.
COMM	Communications (RF)	The radios and modems, antenna(s), cabling, and any other components used to communicate with the ground or other spacecraft. This also may be referred to as Telemetry, Tracking & Communications subsystem.
CPC	Cybersecurity Pathfinder Constellation	A space-based testbed constellation consisting of four LEO satellites that would offer protected experimentation and on-orbit cyber exploitation
EPS	Electrical Power Subsystem	The power collection or production, storage, distribution, and management subsystem.
FMS	Fault Management System	A system that reveals pervasive problems within the spacecraft subsystems. Some of these systems are capable of detecting, isolating, and recovering from in-flight events that may hinder nominal mission operations.
GN&C	Guidance, Navigation & Control	Sometimes referred to as the ODC subsystem, this may overlap with the ADCS. It contains all the sensors and computation necessary to determine and control the spacecraft orbit, including rendezvous and proximity operations. In earth orbit, it often includes a GPS receiver.
GPS	Global Positioning System	A satellite-based navigation system that provides location and time information.
IDS	Intrusion Detection System	A device or software application that monitors a network or systems for malicious activity or policy violations

Acronym	Definition	Context
IP	Internet Protocol	Protocol, or set of rules, for routing and addressing packets of data so that they can travel across networks and arrive at the correct destination.
IPS	Intrusion Prevention System	Network security tool that continuously monitors a network for malicious activity and takes action to prevent it.
IT	Information Technology	Set of related fields that encompass computer systems, software, programming languages, and data and information processing, and storage.
LEO	Low Earth Orbit	Objects that orbit Earth at an altitude of 1,200 miles (2,000 km) or less.
NIST	National Institute of Standards and Technology	NIST's mission is to promote American innovation and industrial competitiveness by advancing measurement science, standards, and technology.
OBC	On-Board Computer	The main computing and data flow controller in the satellite, also referred to as the Command and Data Handling Subsystem (C&DH). In addition to the main microprocessor, this may contain analog-to-digital converters, an internal communications bus or buses, mass memory storage, and attitude control processing.
ODC	Orbit Determination & Control	Sometimes referred to as the GN&C subsystem, this may overlap with the ADCS. It contains all the sensors and computation necessary to determine and control the spacecraft orbit, including rendezvous and proximity operations. In earth orbit, it often includes a GPS receiver.
OT	Operational Technology	Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events.
PC	Personal Computer	A digital device intended for individual use, such as for work, study, gaming, and internet browsing.
Prop	Propulsion Subsystem	The nozzles and thrusters, fuel tanks, piping, valves, and other components used to provide thrust for alerting a spacecraft's trajectory and sometimes controlling attitude.
RDT&E	Research, Development, Test, and Evaluation	Finances research, development, test, and evaluation efforts performed by both contractors and government installations in the development of equipment, material, or computer application software.
RF	Radio Frequency	The frequency of radio waves. In the space system context, RF is used to transmit data between space systems and their ground elements.
SIEM	Security Information and Event Management	A solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

Acronym	Definition	Context
SMS	Structures & Mechanisms Subsystem	The supporting framework of the spacecraft which must be designed to withstand launch vibrations and loads. This is sometimes referred to as the mechanical bus. It may include moving mechanisms such as antenna gimbals and protective doors.
SPARTA	Space Attack Research and Tactic Analysis	A framework developed by Aerospace Corporation intended to provide unclassified information to space professionals about how spacecraft may be compromised due to adversarial actions across the attack lifecycle.
SSC	Stephenson Stellar Corporation	A 501(c)(3) nonprofit cybersecurity research and development organization focused on assuring our nation remains a global leader in the space domain.
SSCR	Stellar Space & Cyber Range	A space based cyber range operated by Stephenson Stellar Corporation
SV	Space Vehicle	A vehicle that operates in space, such as a satellite or spacecraft.
TCS	Thermal Control Subsystem	All the hardware necessary to control the temperature of spacecraft components within their safety and operational limits. This always includes passive components such as radiators and blankets, and also may include active components such as heaters and coolers.
TT&C	Telemetry, Tracking & Communications	The radios and modems, antenna(s), cabling, and any other components used to communicate with the ground or other spacecraft. This also may be referred to as just the COMM.
TTPs	Tactics, Techniques, and Procedures	The behavior of an actor. A tactic is the highest-level description of the behavior; techniques provide a more detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed description of the behavior in the context of a technique.
ZTA	Zero Trust Architecture	A security model that assumes that no user or device can be trusted by default. In the space system context, ZTA is used to improve the security of space systems by reducing the risk of unauthorized access.