A cyber attack-centric view of commercial space vehicles and the steps needed to mitigate

Theresa Suloway, PhD[1] and Samuel Visner[2]
MITRE, Mclean, VA, 22102, USA

Scott Kordella, PhD[3]
MITRE, Mclean, VA, 22102, USA

This paper is provided to inform commercial satellite operators on the workflow of a cyber attacker against their unique ecosystems; it provides techniques and best practices to mitigate steps of an attack. The paper's principal recommendation is the need for robust monitoring of: the ground network, the RF and optical apertures, spacecraft bus, and command and telemetry. The Space ISAC can help members share findings from monitoring activities and provide indications and or signatures of attackers on their systems to the community. Other members of the ISAC can hunt for these signatures on their network to defend and mitigate attacks, thus increasing the security of all commercial space. Progress toward sharing signatures and other threat intel has progressed greatly as membership in the ISAC has increased. Further participation and sharing information among members will increase greatly cyber protection for commercial space.

I. Nomenclature

ELK	=	Elastic Logstash Kibana
ISAC	=	Information Sharing and Analysis Center.
Space Systems	=	System consisting of Space Vehicle and Ground System
Space Vehicle	=	Subset of a Space Systems, Synonymous with Satellite, Spacecraft
API	=	Application Programming Interface
EMM	=	Enterprise Mobility Management
STIG	=	Security Technical Implementation Guides
IT	=	Information Technology
OT	=	Operational Technology

[1] Department Manager, NIST Cyber Programs
[2] Director, National Cybersecurity FFRDC
[3] Director, Space Systems

II. Introduction

The tenants of cybersecurity are availability, confidentially and integrity. These principles decompose into several activities that must be managed by any organization to execute a robust cybersecurity strategy. The processes to implement these ideals have been developed for traditional IT (Information Technology) networks but are still developing for space systems. The paper will examine the architecture of a system devoted to the unique challenges of merging space monitoring data into a traditional IT monitoring strategy. The architecture will address the need to understand: what is on the network (asset discovery), who is on the network, and what is happening on the network. The ability to collect this information is necessary to both identify attacks or attackers in the system and to search for malicious code or activities on critical networks. Traditional IT network monitoring includes identification of malicious Internet Protocol (IP) addresses or a hash of malicious code. These indicators or signatures can typically be obtained from a threat sharing group such as an Information Sharing Working Group (ISWG). Companies that identify these signatures as part of their hunt activities can also share them with ISAC or other government agencies. This sharing activity is crucial to the security of the commercial space industry.

Space presents several unique challenges to the traditional IT monitoring strategy. Space systems, in low and medium orbits, have limited connectivity with the ground network operations center which makes continuous scanning and monitoring difficult. In addition, the traffic between the space vehicle and command center is via Radio Frequency (RF) and threat indicators for RF communications are not IP based. RF threat can have two types, an indicator that is more a Electronic Warfare (EW) aka EMI aka RFI concern would be associated with unusual power or frequency indicators. If the concern is of cyber (which some say incorporates EW/EMI/RFI), the threat indicators will be more along the line of errors, anomalies, rejected commands, rejected hellos, etc. Threats can be detected on the ground if appropriate monitoring is implemented but "signature" is not easily correlated to any threat data currently available from traditional IT monitoring products. Telemetry is a unique feature of space systems which does not lend itself to traditional IT monitoring products. Space system telemetry offers a secondary window into the effects of a cyber attack but not the signatures of the attack. For example, a cyber attacker may introduce malicious code into the space vehicle, but a traditional software scanning product cannot "scan" the space vehicle the same way it would a PC on a business network. However, the effects of malicious code could be seen in anomalous telemetry readings such as battery voltage or payload availability flags. Cyber monitoring data must be correlated with ground system monitoring anomalies to provide space operators a broader situational awareness of a possible cyber event within their space enterprise.

The paper starts with a discussion of a monitoring architecture and activities to implement for asset discovery and scanning. The tools could potentially be used to ingest and correlate the data from both space and ground systems. Section four will discuss monitoring space systems. The next section will examine ground network monitoring and some common Commercial Off the Shelf (COTS) tools can be used to for hardware, software, and credential monitoring. Finally, tools and techniques for monitoring mobile devices and cloud services will be addressed.

III. Monitoring Architecture

In this paper we will use the Lockheed Martin Kill Chain. The first step in the cyber attacker's workflow is to perform reconnaissance on the target system. The attacker wants to know as much as possible about the system (the who what when where how and why) being targeted. The why in this case could include many different reasons. The WHY makes the business case. Is their goal to steal IP to copy and use your hard work to compete? Is it to damage your business model? To know who your customers are? To affect your customers. To destroy your hardware. Your space vehicle? Is the attacker trying to affect your business network (billing, email, etc.) or your OT network (ground stations, satellite ops, etc.)? This reconnaissance usually involves reviewing documentation and network monitoring. To defend a system, the security minded operator should consider a few questions. First, how easy is it to learn about the system? Is critical information in the public domain? Shared with investors or potential clients? It is critical for commercial space operators to protect technical documentation and supply chain documentation associated with their systems and the leased or purchased systems or services they use. Second, how static is the system? Satellite operators have a unique disadvantage in this arena. Tested and qualified flight software and hardware is rarely modified due to concern of on-orbit problems with new versions. However, the longer the attacker has access to your baseline, the longer they can test and identify vulnerabilities. As a best practice, the satellite operator should focus on renewing and upgrading your baseline to mitigate attackers having a long time to find and implement vulnerabilities.

The second step is weaponization. An attack consists of a vulnerability plus an exploit. A cyber-attack requires an exploit to take advantage of a vulnerability. A best practice for satellite operators is to have robust, secure development operations. A vulnerability may not be a Zero Day or technologically advanced malware, it may be inherent buffer overflows or simple logic errors that cause detrimental flaws. Both static and dynamic testing tools for software are available commercially and can be used to identify vulnerabilities during software development and repair before software is loaded onto spacecraft. Many spacecraft operators use open-source software on their systems. These sources should be vetted and tested periodically to prevent vulnerabilities from being built into the space vehicle systems, their ground infrastructure, or both. The ground infrastructure may be more than just a station, might be TT&C apertures that are far away (company might own those links and nodes or might lease them).

The third step in an attacker's workflow is delivery. The attacker must have the ability to deliver their exploit to the space vehicle. Space operators must understand where an attacker can gain access to their network (their attack surface). An example of an attack surface is where the fiber lines come into a building and meet the internal networks. It could also be where business IT systems exchange information with the Operational Technology (OT).

Wireless access to the space vehicle must also be considered as part of the attack surface. For ground uplink and downlink, the attack surface consists of wireless access such as RF antennae, optical link apertures, or both. For the satellite vehicle, the RF antennae as well as the optical link apertures are critical portions of the attack surface. The attack vectors to both the ground system and the satellite are via the internet, RF links, universal serial bus (USB) enabled devices brought in by employees and connected to the network, or email links to malware can be downloaded by users on the satellite network. To mitigate this stage of the attack, a robust monitoring capability for the ground IT and OT network as well as space vehicles is needed. A best practice for satellite operators is to develop a robust monitoring capability by deploying sensors across their network to detect attacks, deploying sensors on the satellite vehicles themselves to detect attacks, and creating out-of-band data streams to monitor end points for intrusion. Monitoring externals such as network traffic, and internals such as keep alive messages, connectivity and as well as commands, and telemetry to identify anomalies is critical for satellite operators to protect their systems. In addition, all aspects of the ground control segment – especially those provisioned by external providers and shared, possibly among several users, are also part of the attack surface and should be instrumented and monitored to detect, block, and mitigate cybersecurity exploits and attacks.

Fig. 1 provides a notional monitoring architecture beginning with the assets, the sensors monitoring the assets and nodes and links, the integration layer which aggregates the data from the sensor suite, the visualization layer used by the Cyber Security Operations Center (CSOC) and finally an external organization such as an ISAC for threat sharing. The architecture of a monitoring system should begin with asset discovery. In the case of commercial space, assets can include, space vehicle, RF apertures, Ground control networks, operator stations, HVAC, mobile devices, and cloud services. While asset discovery of space vehicles is easier to accomplish, the ground network most likely has systems being added and removed regularly. A CSOC should operate on a logically separated network and deploy sensors on the network. These sensors can be configured to flag traffic associated with known bad IP addresses and send alerts to the data integration layer. The integration layer must include the ability ingest data not only from traditional cyber security tools but also from systems monitoring space asset telemetry and links (RF, optical, etc.). Finally, the data must be displayed to the CSOC operators. Most likely the cyber security operators do not have space operations experience so the alerts and flags from space system cyber monitoring sensors must be easily digestible and potentially time correlated with other cyber events on the network. CSOC engineers should be trained and aware of the entire business model so they know what is critical, etc. and that they are collocated / on the same floor as the core space ops team. Finally, anomalies or other threat information can be shared with the Space ISAC.

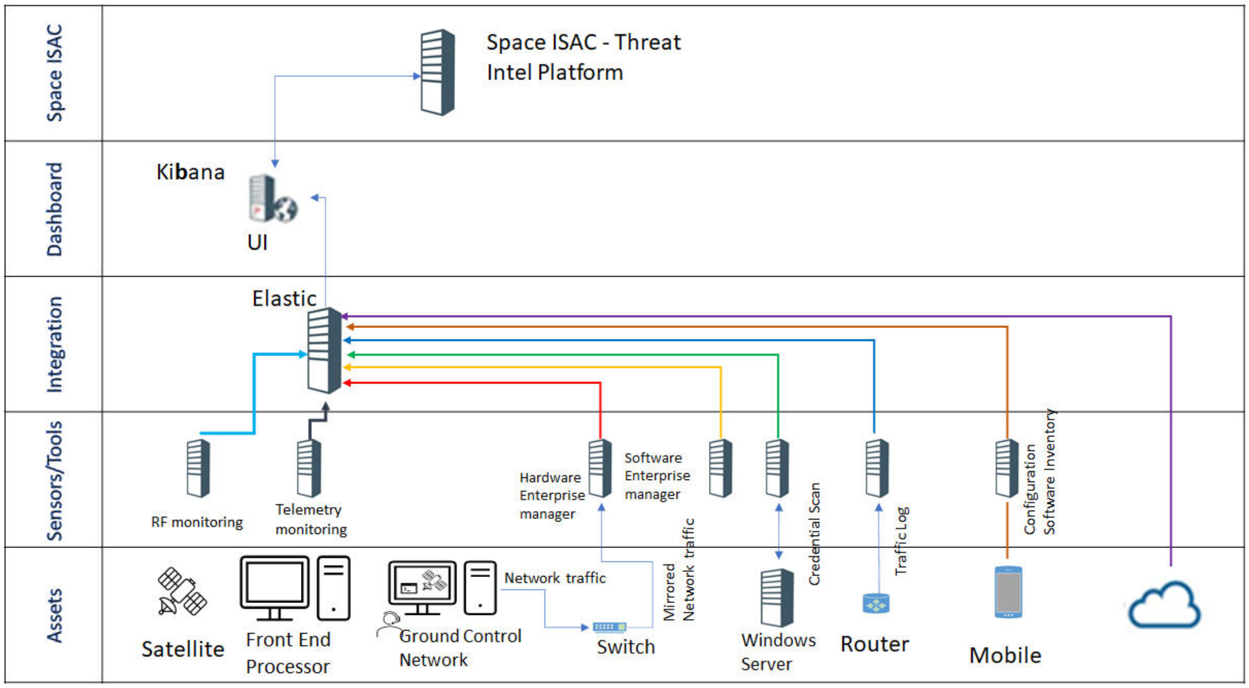

Fig. 1 Monitoring Architecture for Notional Space Operator Organization

The fourth step in the attack is exploitation. At this stage, an attacker has gained access to the vulnerable target and is attempting to create a presence on the system. To mitigate this aspect of an attack, satellite operators should ensure the computers or nodes on the network are hardened. Hardening a node can involve using a secure operating system and employing robust access controls. Security best practices such as role-based access control and host-based access control are also helpful. In addition, tools to detect exploitation on both ground and space systems are encouraged. Space system operators should monitor satellite bus traffic, e.g., MIL-STD1553 or SpaceWire, for intrusion or for evidence of malicious commands. Sensors onboard the space vehicle and bandwidth to send that sensor information to the ground would be required to monitor satellite bus traffic and send that information to the ground.

The final steps in the attack is Installation, Command and control and Actions. It is important to realize an attacker may not want to cause an effect immediately after gaining access to the system, an attacker may want to create a persistent presence on the system to hold the system at risk until an opportune time. Commercial satellite operators should purposely conduct activities to deny potential persistence on their systems. This can involve reinstallation of operating systems on ground systems and space vehicles on an aperiodic basis. Satellite operators may also take advantage of cryptographic file verification, which will deny access to attackers who have access to the network. Satellite operators must have a plan for compromise and how to recover from a breach. These actions and lessons learned are critical to share with the Space ISAC to improve the resilience of commercial space, especially with the complex interdependent support across multiple companies worldwide.

IV.   Spacecraft Monitoring

Space Vehicles are complex systems consisting of their own internal data bus (1553, SpaceWire or others), major subsystems such as attitude determination and control systems, and finally payload subsystems. Dependent on orbit, altitude, and limited bandwidth to the ground command center, a continuous data feed of satellite bus traffic monitoring is not practical. Telemetry offers one of the only insights into what the vehicle is experiencing including cyberattacks. Telemetry monitoring API for the integration layer tools such as Splunk are not know. Considering many space systems are custom, a unique API should be considered to allow satellite operators and cyber security operation engineers to interpolate cyber issues and space vehicle anomalies. Using time stamps to correlate spacecraft anomalies with cyber alerts. Space anomalies are common, however a space anomaly associated with a cyber intrusion alert may be less common.

V. Ground Network Monitoring

A commercial space operator network typically consists of switches to route traffic through the internal network. These switches should be configured to mirror the network traffic so it can be sent to hardware and software enterprise managers for monitoring. COTS tools such as are Forescout Enterprise manager and IBM BigFix can perform hardware and software management functions. BigFix collects and reports configuration security checks based on continuous fixlet evaluation. An agent is installed on every machine in the network communicating with the BigFix server. Security Technical Implementation Guides (STIGs) can be selected in BigFix to evaluate data returned by the fixlet and deviations are reported accordingly. The operator intent of these tools is the ability to initiate asset scan discovery and raw software inventory as well as configuration scans. These tools can be configured to perform a comparison between desired configuration state and current configuration state. Asset identification data and out of date configuration data can then be sent to a data aggregation tool such as Splunk or the ELK stack to be addressed by CSOC personnel. It is important to maintain the configuration of software tools as unpatched systems contain known vulnerabilities can be exploited by attackers. Credential scans are another important tool in the fight against cyberattack. Credentialed scans are scans in which the scanning computer has an account on the computer being scanned allowing the scanner to do a thorough check for problems that cannot be seen from monitoring network alone. As an example, tools such as Tenable Nessus can be used to perform this function. Routers manage traffic between devices or networks and some routers may have the added functionality of facilitating a wireless access point or broadband modem, making them more useful than switches. System monitoring is important, and several tools can be used to accomplish this including Syslog and Redseal.
Syslog stands for System Logging Protocol and is a standard protocol used to send system log or event messages to a specific server, called a syslog server. It is primarily used to collect various device logs from several different machines into the CSOC for monitoring and review.

A. Mobile and Cloud

Surprisingly, mobile devices can be used as part of the command and control network for satellites in orbit[4]. This may grow as satellites proliferate and business models change and require rapid changes in commanding based on customer needs. This leaves a unique challenge for cyber security operators of space systems. A enterprise mobility management (EMM) is a mobile management solution enables enterprises to secure data on employee's personal devices and corporate owned devices. MobileIron or MaaS360 are tools used in support of monitoring of mobile devices on the network. A client of these tools must be downloaded on to the mobile unit to monitor these systems. These tools can conduct configuration software inventory scans and report the results to the integration tool.

Cloud services are becoming increasingly popular for commercial space. Cloud services such as Amazon Web Services and Microsoft Azure are becoming increasingly popular for commercial space. Tools such as Cloud Security Alliance's (CSA) "*Top Threats to Cloud Computing, The Egregious 11*"[5] and MITRE ATT&CK Cloud Matrix[6] can be used to address this different threat surface and novel vulnerabilities. Some of the unique challenges associated with cloud computing are multi-tenancy, identify and access as well as shared vulnerabilities. It is important to note security is a shared responsibility between the user and the cloud service provider and data discover and analysis tools must be understood.

VI. Conclusion

This paper presents the stages of a cyber-attack against a space vehicle, ground network and business IT infrastructure and how a robust monitoring capability is essential to defending against these events. The monitoring

[4] https://www.captechu.edu/blog/how-to-control-a-satellite-with-your-mobile-phone
[5] https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven
[6] https://attack.mitre.org/matrices/enterprise/cloud/

capability should be provided by a CSOC integrated within a commercial space operator’s operations center. The organization’s CSOC must begin with identifying what is on the network to include operational technology such as satellites, front end processors, RF apertures, computer assets, business networks, mobile devices, servers and cloud assets. Sensors should be deployed throughout the enterprise to monitor traffic (IP as well as RF and telemetry). These usually stovepiped data need to be aggregated to identify a potential cyber threat nexus forming within the space ecosystem. Sensor fusion or tipping and queuing based on time stamps of anomalous events is critical for the commercial space operator to stay inside the Observe, Orient, Decide, Act (OODA)[4] loop of an attacker. There is substantial work needs to be performed to make this data fusion a reality. While some cybersecurity data integration tools have API allowing them to integrate with hardware, software and configuration tools, these API do not exist or are not known by the authors. More work needs to be done to create these custom integration tools for space systems. Sharing of threat data gained from a robust monitoring strategy with organizations like the Space ISAC can further strengthen the industry from cyber-attacks.

References

[1] Falco, Gregory. "Cybersecurity principles for space systems." Journal of Aerospace Information Systems 16.2 (2019): 61-70.

[2] Falco, Gregory. "The Vacuum of Space Cyber Security." 2018 AIAA SPACE and Astronautics Forum and Exposition. 2018.

[3] Baylon, Caroline. "Challenges at the intersection of cyber security and space security." International Security (2014).

[4] J.R. Boyd, ―The Essence of Winning and Losing‖, 28 June 1995