Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 09, September-2021

Considerations for Cyberspace Security

James Burrell
Ph.D.
University of Hawaii

***Abstract*— The development of space-based assets and systems provide capabilities and services for exploration, communications, meteorology, geo-spatial, and other national interests. The increased reliance on space-based and enabled services has intensified with the transformation to commercial deployment of space flight operations, reusable launch infrastructure, and small-scale satellite constellations. The economic and market factors associated with innovation, competition, and cost reduction have represented a constant challenge for the design and implementation of highly efficient and secure hardware and software components and systems. Measures of safety, reliability, and resiliency are primary factors in space system engineering that are increasingly challenged by the number and severity of cybersecurity threats. These threats have the ability to impact the integrity and operation of computer, control, and communication systems and networks. These information and communications technology systems are susceptible to cybersecurity threats, vulnerabilities, operations, and attacks that represent a significant risk with the added complexity of remote operation and control in a space-based environment. This paper provides an overview of selected cybersecurity threats with potential considerations to improve reliability, safety, resilience, and security of space systems and networks.**

Keywords—Cybersecurity; space systems

I. INTRODUCTION

The space industry has evolved over the past several decades to support the unique requirements of commercial, civilian, and government applications. In terms of the scale of this industry, in 2021 there were over 4,000 operational satellites in orbit with over fifty percent registered to United States organizations for commercial purposes [1]. The commercialization of the space sector has continued to provide unique opportunities and capabilities. These capabilities have also increased the reliance on space-based services and require a comprehensive assessment of current and evolving threats that impact the operation and resilience for space assets and services.

Space infrastructure is divided into three separate categories: ground segment, space segment, and user segments. The ground segment defines a terrestrial station, or network of stations, which provide communication and control center functionality for the space segment. The space segment includes orbital space platforms with payload capabilities. The user segment includes terrestrial, aerial, and orbital systems capable of communication with space segment assets. The reliable operation of space segment assets depends on a complex combination of parameters that include orbital control, position, and power. The disruption of one or more of these elements presents an increased level of risk for the entire space infrastructure. The system wide risk is complicated by a number of factors that include the introduction of specialized technologies, such as miniaturization, hardening, and production combined with a dependency on space-enabled services. The formal assessment and verification of complex systems is acknowledged as a significant challenge [2]. In recognition of increased levels of risk and reliance on critical space based functions that support unique communication, navigation, and sensing capabilities for maritime, aviation, and terrestrial applications, the U.S. Congress introduced The Space Infrastructure Act in June 2021. This legislative proposal included the designation of space as a critical infrastructure with the requirement to establish guidelines for spacecraft and launch vehicles, space-related terrestrial systems and launch infrastructure, production facilities, and information technology systems [3].

Cybersecurity represents an increasingly important component for the safe and reliable operation of systems and networks in the space, ground, and user segments. The criticality of these systems require the assessment of threats and risks that have a significant effect on information, communications, and control system technologies. Computer network operations that involve targeted actions or activities could result in a range of denial and disruptive effects that increases the level of importance related to cybersecurity. The protection of assets and systems rely on a combination of physical and cyber security considerations that address system and segment specific threats with risk profiles for space operations.

The information technology and security fields have a substantial number of professional certification and training programs offered by vendors, organizations, and academic institutions. The increased focus on space-based cybersecurity issues has resulted in establishment of specialized certifications, to include the International Society of Space Security Specialists (IS4) Certified Space Information Security Manager (CSISM), Space Electronic Warfare Certificate (SEWC), Certified Space Intelligence Analyst (CSIA), and Space Policy and Law Professional (SPLP) [4]. A critical requirement to consider for the evaluation of cybersecurity of space system development, operation, and management includes the impact that proposed security mitigation measures could have on safety, reliability, and resiliency.

The further development of national and international standards specifically related to space operations are important to establish and maintain a level of acceptable practices by commercial and government organizations.

II. SPACE ENVIRONMENTAL CONSIDERATIONS

The space segment represents a unique operating environment for computer and electronic systems, which begins at an altitude of approximately 130 kilometers, and

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 09, September-2021

introduces effects that impact the reliable operation of space-based systems [5]:

- Atmospheric effects
- Electromagnetic radiation
- Charged particle emission
- Solar flares
- Temperature and thermal radiation effects
- Vacuum effects
- Gravity and micro gravity effects
- Micrometeoroids and object collision hazards

These are examples of environmental conditions that can have severe impact on unprotected surfaces, sensors, and components. The effects of these conditions primarily impact physical space structures, but are important to consider the potential impact on electronic and computer components, devices, and systems

III. SECURITY CONSIDERATIONS

The attack surfaces for space systems encompass ground and space-based environments that provide development, production, and implementation of operational services. The ground-based segment includes systems and services for launch infrastructure and control of space-based assets for space transport vehicles, satellites, and other orbital components. The space-based segment also includes actual orbital vehicles and systems operating in the space environment. The computer and control systems used in legacy space-based systems operated on specialized hardware, operating systems, and application software. These space-based computer systems had limited processing and memory capacity that required the majority of the processing to be performed by ground segment computer systems. The NASA Space Shuttle Program adopted a Data Processing System (DPS) that included general-purpose computers (GPC), data bus network (DBN), multifunction displays, and mass memory units (MMU). The DPS consisted of five GPCs, each with a central processing unit (CPU) and a custom input/output processor (IOP) [6]. The design also included data redundancy functionality where the MMU stored a backup of the Primary Avionics Software System (PASS), Backup Flight System (BFS), Display Electronics Unit (DEU), and engine controller software [6].

The National Aeronautics and Space Administration (NASA) PASS Project instituted processes that were utilized for over three decades to deliver highly reliable and resilient software for critical flight and control systems [7]. PASS provided a framework for identifying software errors using trusted software development tools and code inspection and review processes [8]. These processes included quality measures and error detection elements that required re-inspection of software modules when over 10% of the non-commented source code was changed [8]. In comparison, the latest SpaceX Falcon rocket, Dragon capsules, and Starlink satellites incorporate foundations of the Google Chrome browser and a variation of the Linux operating system capable of supporting reliable real-time operations [9]. As a result, these systems incorporate open-source software components in a software development environment with a significant level of programming expertise.

The complexity of hardware and software configurations increases the probability of unidentified programming and execution errors that could remain undetected until a critical mission event or failure occurs. The system design, development, and implementation of ground and space segment hardware and software elements are primarily produced in ground segment facilities. This provides the ability to apply software development, evaluation, and validation methods to the pre-launch deployment of space segment hardware and software systems. This also introduces significant concerns related to supply chain and insider threat security considerations. The application of security incident and event management (SIEM) and threat modeling is a fundamental consideration for assessment and evaluation of cybersecurity risk and critical security controls for effective system wide enterprise risk management.

IV. PHYSICAL THREATS

The potential for physical threats exists in the ground, space, and user segments. The space segment has unique environmental conditions that impact control, sensor, and computer systems and require specialized design, materials, and manufacturing processes to provide high levels of reliability and resilience. The recognition of physical threats is an important consideration for the evaluation of cybersecurity threats, due to the interdependencies that exist between physical and cyber systems. Examples of selected physical threat categories, segment, and impact factors are provided in Fig. 1.

TABLE I. SELECTED PHYSICAL THREAT CATEGORIES AND IMPACT

THREAT CATEGORY	SEGMENT			IMPACT		
Physical	Ground	Space	User	Interference	Disruption	Destruction
Supply Chain	■	■	■	■	■	
Physical Access	■		■	■	■	■
Environmental	■	■	■	■	■	■
Electronic/Electromagnetic /Optical Disturbance	■	■	■	■	■	
Electronic/Electromagnetic /Optical Attack	■	■	■		■	■
Collision/Impact		■			■	■

The level of impact on infrastructure segments includes consideration for cyber physical systems the unique aspects of the space segment.

V. CYBER THREATS

The cybersecurity environment encompasses the design, development, verification, and implementation processes for hardware, firmware, and software. The majority of cyber threats exist in ground, space, and user segments, where physical proximity and access to computer and data storage systems may not be possible in space and user segments. Communication and control systems for space transport and satellite vehicles include software-based components that may introduce threats and vulnerabilities to these systems. Cybersecurity for space systems requires continuous evaluation methodology that includes processes to maintain and evaluate the confidentiality, integrity, availability, authorization, and non-repudiation of systems and data.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 09, September-2021

Examples of selected cyber threat categories, segments, and impact factors are provided in Fig. 2.

TABLE II. SELECTED CYBER THREAT CATEGORIES AND IMPACT

THREAT CATEGORY	SEGMENT			IMPACT		
Cyber	Ground	Space	User	Confidentiality	Integrity	Availability
Supply Chain	■	■	■	■	■	■
Insider Threat	■	■	■	■	■	■
Software Vulnerabilities	■	■	■	■	■	■
Software Execution	■	■	■		■	■
Software Update	■	■	■		■	■
Data and Communications	■	■	■	■	■	

The identified cyber threats impact all infrastructure segments at different levels based on the characteristics of the specific threat and consideration of threats in the design, development, manufacturing, and deployment processes and methods.

A. Supply Chain

The global supply chain provides advantages for product development, manufacturing, and delivery. The supply chain for information and operational technology includes hardware and software components, devices, and modules that are incorporated into end user systems and products. In the development of critical systems, supply chain quality, reliability, and security are important factors that have collective impacts on these systems. A supply chain compromise may occur at any stage of the process, to include the alteration, injection, or removal in hardware and software components, where the identification and detection become increasingly difficult to detect and validate in a global supply chain environment. In certain cases, the undetected introduction of counterfeit products could represent a significant concern for the reliability, safety, and security of space industry components and systems.

B. Insider Threat

The concept of insider threat involves the potential for an individual, with authorized privileged access to knowledge or information, to intentionally or unintentionally disclose, cause damage, or otherwise degrade the operation or value of an organization. The activity could include theft, disclosure, or sabotage that impacts business operations, human capital, information technology, or other critical assets. A complicating factor is the ability to identify potential insider threat conditions with the expanding number of employees, contractors, and associates within organizations that have access to information and information management systems. Insider threats have been identified and recognized as a significant issue for cybersecurity and the detection, detection, and prevention requires a comprehensive multi-tiered approach that examines a combination of technological, physiological, and behavioral based information and metrics [10][11].

C. Software Vulnerabilities

A software vulnerability represents an error in programing syntax, structure, or execution of a program code segment. A vulnerability could include the existence of an error condition derived from a syntactical inaccuracy or complex fault in procedural or conditional logic encountered during the program execution. The identification, evaluation, and mitigation of software and firmware vulnerabilities require the evaluation of development activities and processes that includes third party and contractor contributions. The cybersecurity risks posed by software-based vulnerabilities are especially important in industrial and critical infrastructure environments where the integration of secure software development practices is recommended to mitigate the number and severity of vulnerabilities [12].

D. Software Execution

A trusted execution environment provides an enhanced level of confidentiality with integrity protection against privilege level escalation and compromise of operating system software. A trusted execution environment provides a standards-based approach that incorporates encryption, verification, and isolation techniques to address the complexity and variations in operating system configuration and implementations that introduce potential security vulnerabilities. An approach utilized for space and avionics application requirements include the integration of control and data management functions into a single computer platform executing a real-time operating system [13].

E. Secure Update

The integrity of the computer system initialization and firmware update processes represents a critical requirement for mission critical computer system and devices. A secure initialization process verifies the authenticity and integrity of critical operating software and data [14]. Modern secure systems have also implemented measures that include code signing from a trusted authority that prevents the execution of software versions that may contain known error conditions or security vulnerabilities. The establishment of a secure software update process provides a critical level of protection against the remote installation of unauthorized versions of firmware, operating system, or application software for critical systems.

F. Data and Communications

The confidentiality of stored and transmitted data for certain space operations is an important security requirement to prevent the unauthorized inspection of sensitive information. The decision to implement advanced security methods to provide data security is primarily based on the sensitivity of the data and design constraints for the particular system. An additional consideration includes the effect of electronic, electromagnetic, and optical disturbances on the integrity and availability of data and communications. These disruptive effects could exist in ground, space, and user segments in addition to the wireless communication environment between these segments.

VI. CYBERSECURITY CONSIDERATIONS

The development of processes and methods to address potential risks is a critical consideration for confidentiality, integrity, and availability of space systems that potentially impact the operation and resilience of any information technology system. The management of potential threats to the security of space systems requires approaches that are complementary to current information technology practices and safety considerations. These potential approaches could include the selection and management of appropriate controls that represent a combined approach to safety and cyber security that is consistent with threat, vulnerability, and impact

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 09, September-2021

prioritization. Selected considerations for each of the specified threats are presented as potential options to improve the cybersecurity of space information and communication technology systems in Fig. 3.

TABLE III. SELECTED CYBER THREAT CONSIDERATIONS

THREAT CATEGORY	CONSIDERATION	IMPACT		
Cyber	Description	Confidentiality	Integrity	Availability
Supply Chain	Supply Chain Management	■	■	■
Insider Threat	Insider Threat Management	■	■	■
Software Vulnerabilities	Secure Software Development	■	■	■
Software Execution	Secure Boot and Trusted Execution Environment		■	■
Software Update	Secure Software Update		■	■
Data and Communications	Secure Data and Protocols	■	■	

A. Supply Chain Management

The production of modern information and operational technology products depend on a complex network of distributed global supply chains that provide cost effective solutions [15]. The management of supply chain risks for cybersecurity of space systems is included as a principle in the U.S. Presidential Memorandum on Space Policy [16]. This directive requires product traceability, use of trusted supplies, and risk mitigation measures. The National Institute of Standards and Technology (NIST) developed the Cyber Security Chain Risk Management (C-SCRM) as a process of identifying risks that occur at all stages of the process and potential resultant vulnerabilities [15]. There have also been recent developments in the application of artificial intelligence for supply chain management that aligns with business management models [14].

B. Insider Threat Management

The management of insider threats for cybersecurity of space systems is included as a principle in the U.S. Presidential Memorandum on Space Policy [16]. This directive recommends the use of practices that align with the NIST Cybersecurity Framework (CSF) to reduce risks from a number of sources that include insider threats. The NIST CSF is a framework developed to assist in the reduction of cyber related risks to critical infrastructures, based on standards, guidelines, and best practices [18]. The application of artificial intelligence has been an effective method for identifying network security anomalies and potential indicators of insider threat activities.

C. Secure Software Development

The quality and reliability of software applications is commonly evaluated with a quality assurance process. A code review is a software quality assurance process that involves an independent automated or manual review of source code. A secure code review methodology includes a focused examination of the entire software development cycle to identify vulnerabilities that impact the security of software application [19]. Modern software development methods, such as development and operations (DevOps), provide reduced development time with high-quality results. This methodology has been extended to development, security, and operations (DevSecOps) with the integration of security at all stages of the development process to produce more secure software products. In 2019, NIST announced the Secure Software Development Framework (SSDF) based in part on established secure development best practices of numerous organizations [20]. This framework specifies criteria for risk mitigation methods to include software inspection, third-party verification, and compliance. A significant recommendation presented in this framework is the requirement for performing a continual assessment to identify, analyze, and remediate cybersecurity risks.

D. Secure Initialization and Trusted Execution Environment

A secure initialization process provides authentication and verification methods to prevent the substitution or alteration of valid system software and data. An example of a secure initialization process is described in the Apple iOS Security Guide that uses cryptographically signed components to validate the integrity of the process with a verifiable chain of trust for the boot loader, kernel, kernel extensions, and baseband firmware [21]. This security architecture limits the installation and execution to current versions of authorized code. A trusted execution environment establishes a separate zone where software can be executed and protected against attack methods that occur after the completion of the initialization process.

E. Secure Software Update

The ability to gain unauthorized or unauthenticated remote access to information and communication devices and stored data represents a significant cybersecurity risk. A NASA Space Shuttle system document described a process where memory contents could be updated during flight operations to replace the existing data at a specified memory addresses [9]. A secure software update process prevents the installation of unauthorized system software updates, which is the primary method, utilized to upgrade software components on unattended or remote systems that includes systems in the space and user segments.

F. Secure Data and Protocols

The security of space-based information and communication systems is based on a range of requirements and design considerations. The design consideration for security requirements in ground, space, and user segments are significantly different based on the specific environment and resource availability. An approach to security known as security through obscurity applies to earlier space systems. The identification of major vulnerabilities in the space and user segments include hard-coded credentials and insecure communication and authentication protocols that represent significant risk to interconnected systems and networks [22]. The incorporation of secure data storage and communication protocols include cryptographic techniques and methods to protect the confidentiality and integrity of stored and transmitted data. The use of encryption and secure protocols are effective methods to protect both stored and transmitted data. There are advanced communication techniques designed to mitigate the impact of electronic, electromagnetic, and optical disturbance that affect the integrity and availability of transmission and reception that include alternate frequency selection and anti-jamming countermeasures. Secure cryptographic and advanced communication techniques require increased processing, storage, and power requirements

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 10 Issue 09, September-2021

that represent critical design considerations for resource-constrained devices used in the space and user segments.

VII. CYBERSECURITY SPACE POLICY

The commercialization of the space sector presents an added complexity with the involvement of public and private sector organizations including different nation states. The development of a comprehensive regulatory framework that includes public private collaboration, information sharing, and international cybersecurity norms are required to assist in the coordination and de-confliction of policy issues. An example of the regulatory complexity in the United States includes the number of federal agencies with regulatory or enforcement authority for the space sector: Department of Commerce (DOC), Department of Homeland Security (DHS), Federal Aviation Administration (FAA), Federal Communications Commission (FCC), and National Aeronautics and Space Administration (NASA). In addition, federal agencies have been created specifically to address national space security and superiority missions to include U.S. Space Force and U.S. Space Command. The mission of the U.S. Space Force is to provide organization, training, and equipment to protect U.S. interests in the space environment and the U.S. Space Command provides counter-space capabilities that guarantee continued access to the space environment [23] [24]. The international access and use of the space environment requires multinational coordination in a number of different areas to include security, law, and policy.

CONCLUSION

The space industry has advanced the field of information and communication technologies, which has enabled and supported critical functions for the space and other industry sectors. These advancements were critical to the enablement and support for current and emerging space-based functions. As with many industry sectors, there have been major cybersecurity vulnerabilities identified in space industry that represent significant threats to electronic and computer-based systems. This paper presented several examples of cybersecurity-based threats and included considerations for supply chain, insider threat, secure software development, trusted computing environments, and communication security. These examples demonstrated the complexities related to the identification, detection, and mitigation of cybersecurity risks. A current trend in the commercial space sector is to adopt, adapt, and integrate industry standard computing technologies into space systems. This approach optimizes business operations related to hardware and software development time, cost, and workforce availability. There are also security implications related to the level of security improvement and potential vulnerabilities associated with new attack surfaces. The ability to effectively identify, assess, and mitigate cybersecurity threats for space systems will require constant assessment and mitigation for the combined reliability, safety, resilience, and security of space systems and networks.

REFERENCES

[1] Union of Concerned Satellites, “Satellite Database,” May 01, 2021. https://www.ucsusa.org/resources/satellite-database.
[2] C. Maple et al., “Security-Minded Verification of Space Systems,” in 2020 IEEE Aerospace Conference, Big Sky, MT, USA, Mar. 2020, pp. 1–13.
[3] T. Lieu, “H.R.3713 - 117th Congress (2021-2022): Space Infrastructure Act,” Jun. 04, 2021. https://www.congress.gov/bill/117th-congress/house-bill/3713
[4] International Society of Space Security Specialists, “IS4 Certification Programs.” https://is4.org/certification/
[5] U.S. Federal Aviation Administration, “Advanced Aerospace Medicine-Section III-4.1.2 The Space Environment” U.S. Federal Aviation Administration technical report, April 11, 2018.
[6] N. G. Leveson, “Software and the Challenge of Flight Control.” http://sunnyday.mit.edu/papers/shuttle-chapter-final.pdf
[7] C. Hickey, A. Klausman, B. Loveall, and J. Orr, “The Legacy of Space Shuttle Flight Software,” in AIAA SPACE 2011 Conference & Exposition, 2011, p. 7307.
[8] U.S. National Aeronautics and Space Administration, “Space Shuttle Program Primary Avionics Software System (PASS) Success Legacy - Major Accomplishments and Lessons Learned Detail Historical Timeline Analysis,” NASA Technical Report.
[9] S. Shankland , “SpaceX rockets fly with software you can find on your Android phone – CNET,” Jun. 09, 2020. https://www.cnet.com/news/spacex-rockets-fly-with-software-you-can-find-on-your-android-phone/
[10] Yaseen, Q.; Panda, B. Insider threat mitigation: Preventing unauthorized knowledge acquisition. Int. J. Inf. Secur. 2012, 11, 269–280.
[11] R. A. Alsowail and T. Al-Shehari, “A Multi-Tiered Framework for Insider Threat Prevention,” Electronics, vol. 10, no. 9, p. 1005, 2021.
[12] T. E. Gasiba, U. Lechner, and M. Pinto-Albuquerque, “CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments.”
[13] S. Pinto, A. Tavares, and S. Montenegro, “HYPERVISOR FOR REAL TIME SPACE APPLICATIONS,” p. 14, 2016.
[14] Apple Inc., “Apple Platform Security.” https://support.apple.com/guide/security/welcome/1/web
[15] U.S. National Institute of Standards and Technology, “Cyber Supply Chain Risk Management,” May 24, 2016. https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management
[16] U.S. Presidential Memorandum, “Memorandum on Space Policy Directive-5—Cybersecurity Principles for Space Systems.” https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/
[17] P. Helo and Y. Hao, “Artificial intelligence in operations management and supply chain management: an exploratory case study,” Production Planning & Control, pp. 1–18, Apr. 2021.
[18] U.S. National Institute of Standards and Technology, “Cybersecurity Framework,” NIST, Jul. 14, 2021. https://www.nist.gov/cyberframework/getting-started
[19] MITRE, “Secure Code Review,” Aug. 2013. https://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/secure-code-review
[20] U.S. National Institute of Standards and Technology, “Secure Software Development Framework,” Feb. 25, 2021. https://csrc.nist.gov/projects/ssdf
[21] Apple Inc., “iOS Security Guide,” Jan. 2018,” p. 82, 2018.
[22] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, and A. Davis, “Cyber security in New Space,” Int. J. Inf. Secur., vol. 20, no. 3, pp. 287–311, Jun. 2021.
[23] U.S. Space Force, “Mission.” https://www.spaceforce.mil/About-Us/About-Space-Force/Mission/
[24] U.S. Space Command, “Commander’s Strategic Vision.” https://www.spacecom.mil/Mission/Commanders-Strategic-Vision/