Engineering and Assessing Cybersecurity for Space Systems

Pedro Sousa[1], João Cunha[1], Nuno Silva[2]
[1]*Polytechnic Institute of Coimbra, Coimbra Institute of Engineering,*
Rua Pedro Nunes, 3030-199 Coimbra, Portugal
Emails: {a21260376, jcunha}@isec.pt}
[2]*Critical Software SA, Parque Industrial de Taveiro, Lote 49, 3045-504 Coimbra, Portugal*
Email: {nsilva@criticalsoftware.com}, Tel.: +351 932574030 (Presenter)

ABSTRACT

This paper provides analysis of the main challenges and considerations concerning cybersecurity for space systems, highlighting the urgent needs for collaborative efforts among stakeholders to safeguard critical infrastructures that compose the space domain. We distributed a survey to experts working in the space industry, focusing on cybersecurity challenges and solutions for space systems, pinpointing vulnerabilities, threats, and mitigation strategies. This approach provided us with an empirical basis on which we can work to find solutions and possible directions to ensure cybersecurity soundness for space systems. Additional feedback will be incorporated in the database, as well as the outcomes of recent literature studies about cybersecurity. All this research will lead to proposals for systems/software engineering, assessments and space standards improvements in order to ensure appropriate cybersecurity requirements and implementation in space systems.

KEYWORDS: Cybersecurity, vulnerabilities, threats, mitigation strategies, space systems, space software, engineering, verification and validation

1 INTRODUCTION

The significance of ensuring the security of space systems has become increasingly paramount as space exploration continues to advance. In the early years of space exploration, the development of space systems adhered to the principle of "security through obscurity", implementing rigorous confidentiality measures to impede potential threats to adversaries' military capabilities. However, with the advent of technological advancements, especially in computing, the number of satellites orbiting Earth has seen a substantial increase, consequently expanding the attack surface for cyber attacks.

Despite ongoing efforts to enhance the cybersecurity of critical infrastructures, space systems have often been overlooked, and it is only in recent years that cybersecurity considerations have gained attention. Initially, NASA standards began incorporating cybersecurity measures, and more recently, the European Space Agency (ESA) has included the cybersecurity topic in its standards from the European Cooperation for Space Standardization (ECSS) ([1], [2]). This paper addresses this critical gap and lays the groundwork for the development, verification, and validation of secure space systems and software engineering. It aims to identify potential threats, vulnerabilities, and methodologies to ensure cybersecurity while offering potential contributions to the development and standardization of space systems through verification and validation (V&V).

This section introduces the subject, followed by Section 2 providing a brief background on cybersecurity in space systems. Section 3 delves into the most pertinent forms of cybersecurity attacks and vulnerabilities related to space systems. Section 4 details a short survey used to collect data on the topic of space systems cybersecurity, along with some preliminary results. Section 5 concludes the paper and outlines future work, while Section 6 acknowledges the contributions made to this research.

2 BACKGROUND

The shift to digitalization brought about numerous benefits, including heightened productivity, streamlined processes, and enhanced product quality. However, it also introduced significant vulnerabilities as systems became interconnected, leaving them susceptible to public access.

The advent of digitalization also ushered in various protocols facilitating communication across networks. While each producer and operator of industrial control systems had their own protocols, believed to be secure, they were nonetheless prone to compromise. The absence of cybersecurity standards and regulations further compounded the security challenges faced by space systems.

Presently, these challenges centre around the intricate nature of space systems, the lack of robust enforcement of cybersecurity standards and regulations, intricate supply chains, lengthy asset life cycles, Commercial-off-the-shelf (COTS) components, and resource constraints [3].

3 ATTACKS AND VULNERABILITIES OF CYBERSECURITY FOR SPACE SYSTEMS

As relevant examples, publicly know, extracted from a literature analysis, there have been numerous cyberattacks / cyberthreats with severe impacts. Some types and consequences of these attacks are listed in the following subsections.

3.1 Spoofing

Spoofing is a deceptive tactic that involves masquerading as a trusted source to gain access to sensitive information or networks.

GPS satellite spoofing already occurred. In September 2011, Iranians successfully captured an American RQ-170 drone by manipulating the GPS signal coordinates (spoofing), leading it to land within Iranian territory [3].

3.2 Jamming

Jamming is the intentional interference with communication signals, disrupting or preventing the normal functioning of radio, radar, or other electronic systems.

Given the conflict between Russia and Ukraine, there has been a notable increase in attacks targeting electronic systems. An incident of note occurred when SpaceX made its Starlink system (a satellite internet constellation) available for use by the Ukrainian population and military. To disrupt Starlink, methods like jamming and voltage fault injection, were used. This latter attack method was demonstrated at a conference in Las Vegas by Lennert Wouters, a cybersecurity researcher. He demonstrated an attack on a Starlink user terminal (UT) using a simple $25 chip, allowing him to infiltrate the dish and exploit vulnerabilities within the Starlink network [4].

3.3 Solar radio burst

A solar radio burst is a sudden and intense release of radio frequency energy from the Sun, typically associated with solar flares or other solar eruptive events.

Recently, the sun emitted the strongest solar flares in the last 7 years. This is a powerful explosion within the sun surface that expel great quantities of radiation that effect everything electrical, from electrical grids to disrupting navigation signal in satellites [5]. This is not a cyberattack, but instead a cybersecurity environmental threat that space systems are exposed to.

3.4 Malware

Malware is malicious software designed to harm or exploit computer systems, often by gaining unauthorized access, stealing data, or causing damage to software and hardware.

During Russia's invasion of Ukraine, a malicious software command was directed at the communication provider ViaSat, resulting in the incapacitation of tens of thousands of modems across Europe as unintended consequences. This occurred because the affected modems relied on the same satellite network utilized by the Ukrainian government and military [6].

4 SURVEY AND RESULTS

To comprehensively address contemporary cybersecurity concerns and solutions for space systems, we aim to incorporate expert perspectives on various facets, including existing vulnerabilities and weaknesses, analyses thereof, and the identification of potential solutions and mitigations. TABLE 1 outlines the used survey questions providing a structured overview. The survey was built around several requirements, being the most relevant ones the following:

1. The survey should be short and with simple questions:
2. The survey should contain definitions for cybersecurity terms;
3. The survey should cover the problems, meaning that threats and vulnerabilities of space systems should be collected;
4. The survey should also cover the solutions, including technical solutions, such as technologies, and processual solutions, such as methodologies;
5. The survey should also collect the list of standards currently being used or known;
6. Finally, the survey should allow the experts to provide additional feedback concerning the cybersecurity concerns.

Table 1
Survey of "Cybersecurity challenges and solutions for space systems"

Number	Question
1	List up to 5 of the most common or severe vulnerabilities that you believe affect space or ground systems (or embedded real-time systems).
2	List up to 5 cybersecurity threats that you consider relevant for space or ground systems (or embedded real-time systems).
3	Identify up to 5 Technical Mitigations that are applied or could be applied to prevent cybersecurity problems in space or ground systems.
4	Identify up to 5 Processual Mitigations that are applied or could be applied to prevent cybersecurity problems in space or ground systems.
5	List the standards or cybersecurity resources used to ensure compliance and security of space or ground systems.
6	Select the segment of space systems that do you think are most vulnerable to cybersecurity threats. (Ground, Space or Link/Signal)
7	Any other cybersecurity concerns/trends that you see in the short/middle term (up to 10 years from now) for safety-critical embedded systems, particularly space systems.

The final results of the survey are presented in the following subsections. We received responses from a significant number of experienced space systems engineers (mostly European space engineers, Brazil and US), totaling more than 20 responses. These results are meant for discussion and the final intention is proposed software engineering good practices, processes and tools in order to ensure secure space systems.

4.1 Space Systems Vulnerabilities

A vulnerability is a flaw or weakness in an asset's design, implementation, or operation and management that could be exploited by a threat (e.g. an open or accessible communication protocol).

The main vulnerabilities highlighted by the experts through their responses are (ordered by the most frequently referred to the least frequently referred):

- Access control vulnerabilities.
- Verification & Validation vulnerabilities.
- Communication link encryption/protection vulnerabilities.
- Open-source/libraries/Operating Systems/COTS vulnerabilities.
- Software design not protected against fuzzed inputs.
- Reuse of software/system not thoroughly tested or trusted wrongly.
- Use of tools not mature enough for software development, testing.
- Software bugs with security impact.
- Weak development processes.
- Read & Write operations in memory (stack overflow).
- Insufficient safety and security analysis done in the initial phases (prior to requirements baseline).
- Lack of security assessment and analyses to derive security requirements.
- Ignore code smells and other code rules violations provided by commercial static analysis tools.

4.2 Space systems threats

A threat is a potential for a threat agent to exploit a vulnerability (e.g. external interference in telecommands or telemetry).

The main threats identified by the experts are as follows (ranked from the most frequently referred to the least frequently referred):

- Jamming of communications channel/Satellite.
- Malware and ransomware.
- Distributed Denial of Service (DDOS).
- Middle-man threats in ground operations of space assets.
- Stolen data being on ground stations.
- Space weather/solar storms.
- Insider attacks (e.g. attacking the development/validation environment, software patch to exclude commandability).
- Tampering with source code/binary to introduce accidental or malicious code.
- Supply chain attacks.
- Data security risk (e.g. ground systems critical for processing satellite data are susceptible to cyberattacks, cloud security and other measures could be compromised)
- Prioritizing speed over thorough security practices (design reviews, code analysis, testing) increases the likelihood of vulnerabilities to be explore by threat actors.
- Lack of certification of space systems.
- IP theft (e.g. root causes of the ViaSat incident).

4.3 Proposed technical mitigations

Technical mitigation is the process of applying technical solutions, such as patches, updates, firewalls, encryption, etc., to reduce the risk of a vulnerability being exploited by an attacker.

The most frequently considered technical mitigations, by the experts, are (ranked from the most frequently referred to the least frequently referred):

- Advanced encryption in the communication link and data storage.
- Extensive code analysis (static analysis with cybersecurity rules).
- Intrusion detection mechanisms and tools.
- Proper authentication methods and access control.
- CRCs for all data transmission.
- Secure-by-design approach (Zero trust solutions).
- Eliminate passwords and transition to more secure passkeys for user authentication.
- Implement a stateful firewall to control and monitor all incoming and outgoing traffic, filtering authorized communication and blocking potential threats.
- Regularly perform in-depth penetration testing to identify and exploit vulnerabilities in exposed systems and interfaces.
- Achieve high code quality by eliminating code smells and achieving zero warnings from static analysis tools.
- Implement robust handshake protocols to establish secure connections between ground stations and satellites during data transfers.
- Validated telecommands by hardware or software before execution, mitigating unauthorized commands.
- Utilize certified software development tools throughout the development process.

4.4 Proposed processual mitigations

Processual mitigation is the process of improving the plans, procedures, policies, and practices of an organization to prevent or minimize the impact of a vulnerability or an incident. This can include conducting regular audits, training staff, enforcing security standards, etc.

The most frequently considered processual mitigations, by the experts, are:

- Enforcing security standards (in satellite and ground systems).
- Comprehensive security testing (penetration testing, fuzz testing, out-of-bounds, equivalence class partitioning test, buffer overflow, DoS tests, simulated attacks).
- Cybersecurity awareness trainings to developers.
- Regular independent security audits.
- Follow a Secure Development Life Cycle (SDLC) for application development.
- Define security requirements at the beginning of the project to avoid vulnerabilities.
- Implement vulnerability scans for Open Source Software (OSS) libraries and other third-party software to identify potential security weaknesses.

- Conduct a comprehensive vulnerability assessment of the satellite data center before finalizing requirements**.**
- Implement a maintenance plan that incorporates security considerations (e.g., incident response procedures).
- Provide user manuals and documentation that cover secure installation, operation, and maintenance procedures.
- Implement stricter controls to safeguard information and deliverables throughout the development lifecycle.
- Enforce user authentication for everyone accessing project-related activities. (Zero Trust Model)
  Prioritize a development approach that emphasizes strong security controls at every stage (analysis, design, implementation, testing).

4.5 Standards and other cybersecurity resources

This subsection lists the space related standards and other resources that can be tools to support cybersecurity analysis, development or validation.

The following are standards and resources that have been recommended by the experts who have experience using them in practice.

- NIST (CSF, SP 800) [11]
- ECSS (ECSS-Q-ST-80-10C DIR1, ECSS-Q-ST-80C, ECSS-E-ST-40C DIR) [2]
- ISA/IEC 62443 (for control systems) [12]
- ISO 27000 family (27001 and 27002) [13]
- NTSS (STD-8739.8B, STD-2601, STD-1006A, among others) [1]
- CWE Top 25 [9]
- MITRE tools – ARR&CK, Engage, D3FEND, Caldera [14]
- CCSDS [10]
- ISO 21434 (road vehicles cybersecurity) [15]
- DO-326 (aviation cybersecurity) [16]
- EN50701 (railway cybersecurity) [17]
- SEI secure code standards [18]
- SANS CWE Top-N lists [19]

4.6 Space segment more vulnerable to cyberthreats

According to the experts, the segment that is considered the most vulnerable to cyberattacks/cyberthreats is the ground segment due to the accessibility and existing interfaces, therefore more exposure exists to all kind of attacks (e.g., social engineering, unauthorized access), followed by the link/signal segment, which can also be access through the first one and that allows control of the satellites or unauthorized access to data.

4.7 Other concerns/trends

The community also acknowledges some additional concerns/trends that will affect cybersecurity engineering and assessment over the next years, namely:

- Artificial Intelligence and Machine Learning use in cyber war [7].
- Technical teams acquaintance with cybersecurity concepts, analysis and requirements.
- Political or geopolitical issues, causing cyberwarfare by powerful states/anarchists and climate fundamentalist movements.
- Space debris and physical attacks (e.g. ASAT).
- Cybersecurity certification/legislation might become necessary (as for functional and safety).
- International cooperation (especially in what concerns standards, best practices, methods and tools).
- The arrival of the quantum computer will endanger the currently established encryption algorithms [8].
- Conduct a comprehensive security risk analysis and document all findings.
- Implement threat analysis procedures similar to hazard analysis but focused on identifying and mitigating cybersecurity risks.
- Integrate security considerations throughout the entire development lifecycle, making it an inherent property of the satellite system, similar to how safety is currently treated.

5 CONCLUSION AND FUTURE WORK

There are real threats and vulnerabilities in space systems. Cybersecurity concerns are nowadays getting traction and gaining importance in the systems and software engineering as well as in the verification and validation. For this, we have collected a set of realistic vulnerabilities, threats, mitigations, tools and concerns for the future of ensuring cybersecure space systems. This research will be concluded shortly and a set of processes, techniques and tools, as well as standard recommendations will be defined and discussed with the space systems community.

In what concerns the future work we highlight the following topics:

- Consider literature studies related to cybersecurity practices, methods and tools that are applicable to space systems development and V&V;
- Draft a Cybersecurity for space systems report, including the state of the art and ways forward , and gather further feedback from the space system community;
- Propose a set of best practices, methods and tools for space software engineering and for V&V – and determine also how feasible/applicable they are;
- Propose a set of adjustments/evolutions/recommendations to be considered in space standards in the near future, especially for the European space standards (ECSS);
- We'll need to also manage the threats to validity of the obtained results. Since the consulted experts are not necessarily cybersecurity experts, have different levels of expertise, work in different space systems

segments and have distinct engineering expertise. Also, the knowledge about threats, vulnerabilities, security processes and tools might be limited given the limited maturity of the space domain related to the cybersecurity topics.

6 ACKNOWLEDGEMENT

The authors would like to acknowledge the valuable inputs from all the survey participants so far, as well as the support from Critical Software, SA.

7 REFERENCES

[1] "NASA Technical Standards System", [Online]. Available: https://standards.nasa.gov. [Accessed 27 February 2024].

[2] "European Cooperation for Space Standardization", [Online]. Available: https://ecss.nl. [Accessed 27 February 2024].

[3] G. Falco, "Cybersecurity Principles for Space Systems", *Journal of Aerospace Information System,* vol. 16, no. 2, pp. 1-10, 2018.

[4] Evona, "Elon Musk's Starlink Hacked With $25 Device", 2023. [Online]. Available: https://www.evona.com/blog/elon-musks-starlink-hacked/. [Accessed 26 February 2024].

[5] E. Ralls, "Strongest solar flare in 7 years prompts auroras and satellite warnings", earth.com, 26 February 2024. [Online]. Available: https://www.earth.com/news/strongest-solar-flare-in-7-years-prompts-gps-satellite-warnings-and-aurora-alert/.[Accessed 26 February 2024].

[6] B. N, G. N and F. G, "Space Cybersecurity Lessons Learned from The ViaSat Cyberattack", in *AIAA Ascend*, Las Vegas, 2022.

[7] "Microsoft detected hackers from several countries using its Artificial Intelligence tools", 26 February 2024. [Online]. Available: https://visao.pt/exameinformatica/noticias-ei/mercados/2024-02-15-microsoft-detetou-hackers-usar-as-ferramentas-de-inteligencia-artificial/. [Accessed 26 February 2024].

[8] A. Jackson, "Quantum-safe cryptography with IBM's Michael Osborne", 17 December 2023. [Online]. Available: https://technologymagazine.com/digital-transformation/quantum-safe-cryptography-with-ibms-michael-osborne. [Accessed 26 February 2024].

[9] "CWE Top 25 Most Dangerous Software Weaknesses", 30 November 2023. [Online]. Available: https://cwe.mitre.org/top25/.

[10] "CCSDS Consultative Committee for Space Data Systems", [Online]. Available: https://cwe.mitre.org/top25/. [Accessed 26 February 2024].

[11] "NIST National Institute of Standards and Technology", [Online]. Available: https://www.nist.gov/. [Accessed 29 May 2024].

[12] "ISA/IEC 62443 Series of Standards", [Online]. Available: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards. [Accessed 29 May 2024].

[13] "ISO/IEC 27000 family", [Online]. Available: https://www.iso.org/standard/iso-iec-27000-family. [Accessed 29 May 2024].

[14] "MITRE", [Online]. Available: https://www.mitre.org/. [Accessed 29 May 2024].

[15] "ISO/SAE 21434:2021", [Online]. Available: https://www.iso.org/standard/70918.html. [Accessed 29 May 2024].

[16] "RTCA DO-326", [Online]. Available: https://standards.globalspec.com/std/9869201/rtca-do-326. [Accessed 29 May 2024].

[17] "CLC/TS 50701:2023", [Online]. Available: https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/. [Accessed 29 May 2024].

[18] "SEI CERT Coding Standards", [Online]. Available: https://wiki.sei.cmu.edu/confluence/. [Accessed 29 May 2024].

[19] "CWE Common Weakness Enumeration", [Online]. Available: https://cwe.mitre.org/scoring/index.html#top_n_lists. [Accessed 29 May 2024].