Modeling Information Security Threats for the Terrestrial Segment of Space Communications

Makhabbat Bakyt[1], Khuralay Moldamurat[1], Dina Zh. Satybaldina[1], and Nikolay K. Yurkov[1]

[1] *L.N. Gumilyov Eurasian National University, Astana, 010000, Kazakhstan*

Abstract

This article discusses the modeling of information security threats for the ground segment of space communications. A theoretical analysis of threat modeling is given, including the protection of terrestrial satellite systems. The practical part describes the threat modeling for the ground segment, the organization and evaluation of the seminar on threat modeling.

Keywords

Cyber security, space communications, information security, encryption, aircraft

1. Introduction

Since the launch of Sputnik in October 1957, space technology has played a critical role in the advent of the information age. Today there are many more satellites than mere scientific demonstrations, instead supporting the essential services that define our lives. As the satellite industry experiences a market renaissance, by miniaturizing and lowering launch costs while protecting these systems from cyberattacks, the value of cyberattacks will only increase.

Today, satellite cybersecurity is a disparate and ill-defined topic of critical importance. Contributions spread across disciplines ranging from history and security research to aerospace engineering and astrophysics. This article attempts to highlight these interdisciplinary contributions and systematize knowledge about the security status of space systems [1].

The process begins with the modeling of information security threats for the terrestrial segment of space communications. Characterize threats to space systems into a single matrix linking attackers, vulnerabilities and motives. This model is supported by an exhaustive historical time of satellite incidents. The end result is an empirical and proven basis for those arguing for space systems security research.

We build on this foundation to propose a natural taxonomy for ground segment safety. To do this, we apply our threat modeling process to ensure that the latest technical and academic developments help uncover unresolved issues.

Related to the safety and security of space flights. This includes an explicit presentation of promising research directions in each sub-field [2]. We use this analysis not only to motivate the technical study in this article, but also as a launch pad for future work in the domain.

Proceedings of the 7th International Conference on Digital Technologies in Education, Science and Industry (DTESI 2022), October 20–21, 2022, Almaty, Kazakhstan

EMAIL: bakyt.makhabbat@gmail.com (Makhabbat Bakyt); moldamurat@yandex.kz (Khuralay Moldamurat); satybaldina_dzh@enu.kz (Dina Zh. Satybaldina); yurkov_nk@mail.ru (Nikolay K. Yurkov)

ORCID: 0000-0002-1246-9696 (Makhabbat Bakyt); 0000-0002-3691-6948 (Khuralay Moldamurat); 0000-0003-0291-4685 (Dina Zh. Satybaldina); 0000-0002-2425-3470 (Nikolay K. Yurkov)

2. Theoretical part

Unlike space platforms, which suffer from esoteric equipment and limited access, ground-based systems benefit from a lot of general cybersecurity knowledge. As a rule, satellite ground stations are no different from any other terrestrial network computing systems, and where they differ, remain similar to terrestrial communications systems. Despite the variety of implementations, all ground stations at least consist of radio equipment and a computer that controls the equipment [3]. Usually, the computer runs traditional operating systems with specialized software for satellite communications.

This article used the results of the work of ENU students and teachers on the development and modeling of an intelligent cruise missile control system based on fuzzy logic, the development of a software simulator for controlling a swarm of small satellites, the development and implementation of automated UAV flight algorithms for inertial navigation systems, the coordination of the movement of multi-agent robotic systems, navigation system based on Bluetooth beacons: implementation and experimental evaluation.

On rare occasions, this specialized software has been targeted. For example, in 2000, hackers stole copies of the Exigent software for controlling reverse engineering satellites. Typically, attacks are the by-products of non-targeted intrusions (such as in 1999 when a curious teenage hacker accidentally gained access to NASA's flight control systems). Because of this, very little academic literature has been devoted to the safety of ground stations [4]. However, some unique aspects are worth considering.

First, satellite terrestrial systems almost always represent the last line of defense against payload exploitation. Satellite software and hardware typically follow an "open trust" model, in which the ground station is trusted by all devices on board the space platform. Thus, ground systems represent a single point of failure for missions. In light of this problem, Llanso and Pearson propose the development of redundant stations so that control can be restored if compromised or lost. This is one possible application of the new ground station as a service offering.

Second, satellite terrestrial systems may be located in remote areas with limited access to physical security controls. This is because the main placement considerations are related to signal coverage and access to a particular orbit [5]. Often, few employees will have a regular physical presence on site. Instead, day-to-day operations will be highly automated and controlled remotely from a centralized operations center.

This increases the threat of physical access attacks and is in contrast to many other important information systems.

Table 1

Example of research direction for ground security

Security Challenge	Domain-Related Obstacles	Individual areas of relevant knowledge
A destructive malware or denial of service attack against a ground station can functionally isolate a space mission.	The high cost of equipment means that operators can only have one point of contact with their satellites.	Cloud Safety Distributed / Common sensor networks
A compromised ground station computer can issue a trusted flight control command to the satellite.	Limited in-orbit testing capability means testing often based on the station rather than its user.	PKI and Signature systems Industrial Control System Safety
A backdoor in signal processing equipment hides important data (for example, photos of a certain region, edge).	Heavy use of proprietary protocols and hardware components. A lone point of failure means only attackers need to manipulate data ingestion, not transmission.	Supply chain Safety Signal Treatment

Finally, satellite earth stations are usually the main "bridge" between the terrestrial Internet and satellites. Due to heavy use of remote access, it is difficult for ground stations to completely "air gap". Previous security research has identified numerous exploitable vulnerabilities in ground station software and demonstrated that ground terminals can be easily identified using IOT search engines such as Shodan. Moreover, the relative normality of the ground station equipment means that entry barriers are low compared to other segments.

Typically, traditional corporate security practices are prescribed to protect terrestrial systems. For example, it is possible to conduct a malware audit at a ground station using traditional forensic tools [6]. There are some systems that are unique to the satellite environment and may require a special security regime, such as long range radio equipment. However, our historical analysis has not found a public example of attacks on this equipment and limited academic research into these factors.

Therefore, ground station security is generally considered an extension of traditional IT security. The critical difference often lies in the severity of the potential harm rather than the attack and defense mechanisms. However, this maxim is far from universal. Future offensive security efforts will focus on unique satellite control hardware and software can detect previously overlooked vulnerabilities. A few demonstrative examples of directions for studying these dynamics are given in Table 1.

3. Practical part

The threat modeling procedure had to be tested in a real scenario. Ever since Huld has been developing ground segment software to provide a secure ground segment as a service solution for space projects, it has been chosen as a test shop.

The ground segment as a service solution for Orbitcon was under development.

The goal of the project was to create a Mission Control System (MCS) to meet the needs of new space projects launching and operating small satellites throughout the mission life cycle. The service was based on the cloud. The system supports the Space Link Extension Protocol (SLE) to connect existing ground stations, in addition, its design covered VHF, UHF and S-BAND [7].

The method chosen for the evaluation was action research. Action research aims to solve problems while developing knowledge focused on collaboration and change.

Organization of a Threat Modeling Workshop

The decision to organize the workshop was made instantly after the proposal was received and submitted internally to management. All parties agreed that ground segment threat modeling is beneficial and essential to the success of the project. In addition, the threat modeling procedure can be adapted for other segments of the space industry and offered to customers in the future.

The first step was to draw up a list of participants. People with the following roles were invited:

- product manager;
- developers, three people;
- cybersecurity specialists, 3 persons;
- space specialist; as well as
- managers, three people.

The second step was to choose the date and time of the seminar. The invitation included the scope and purpose of the meeting and the agenda. With so many people involved, it was not easy to find a suitable date, but after the postponement, the event was immediately rescheduled to a new date, which suited all the invitees.

The first problem with the organization of the event arose when the format of the seminar became a subject of discussion. Seminars traditionally work best when all participants meet in person in a conference room with whiteboard access. This helps the general drawing and understanding of the system diagram, and also helps the emergence of new ideas. However, being physically in the same room helps the facilitator

to read participants' body language and gestures and understand if someone is losing interest or strongly disagreeing with something without phrasing it.

Since the team was in different countries and there were international travel restrictions in place during the workshop, it was not possible to meet the participants in person. It was decided to organize the seminar in the format of an online conference.

The choice of platform for the online seminar was a matter that was not considered for long [8]. Since the company used Microsoft (MS) Teams as its internal communication tool, it was chosen as the default option. In addition to choosing a tool for communication, I needed a tool for drawing on a white board or diagrams. For this, the Draw.io tool of the target was chosen as it was free, had a standalone, non-cloud version that included threat modeling diagramming tools. Although it lacked joint functions, but this was not considered critical for the workshop, as some basic collaborative functionality was included in Microsoft Teams.

The duration of the workshop was set at two hours. Shostak's recommendation for small systems was a total of 3–40 hours, the volume of the workshop did not threaten to model the entire system, only part of it. As a basis for the workshop there was an intensive preparation together with the product manager and the system diagram created. This took a significant amount of time and several iterations.

The reason for this was to save time during the workshop.

Workshop

The seminar was divided into two sections. The first part was an introductory presentation of the Threat Modeling Workshop. The method, process, rules and subjects of threats were presented. This was followed by an overview of the system diagram and a brief introduction to the system. This first section took thirty minutes. The second section was reserved for the creative threat discovery and brainstorming phase, which was only interrupted for a five-minute break.

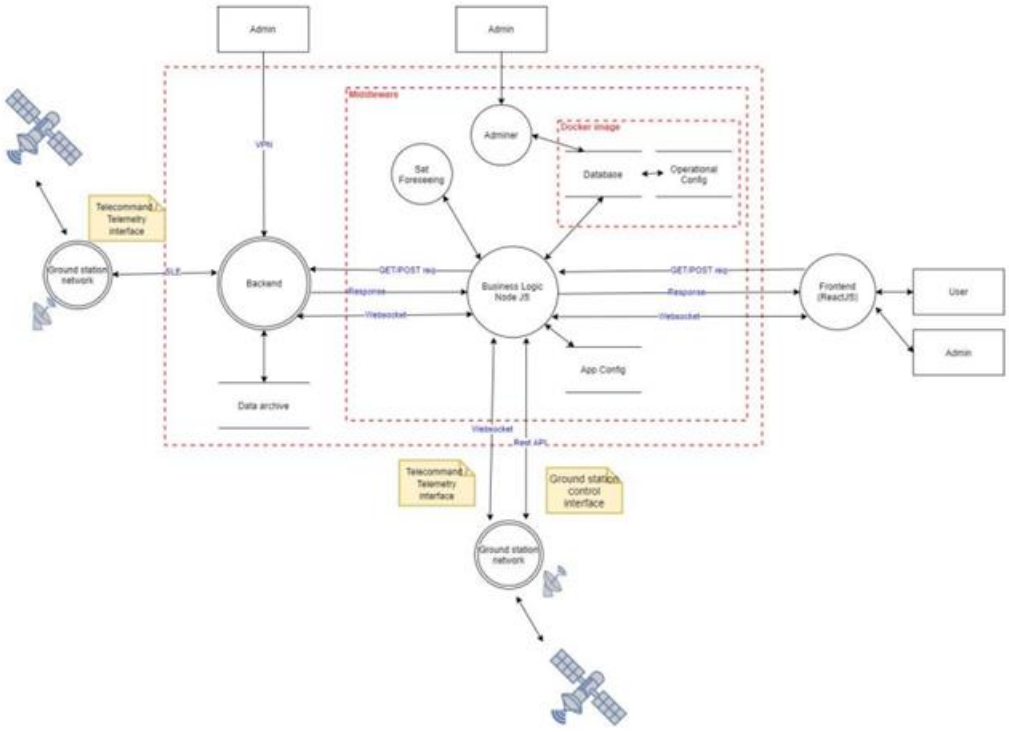

Figure 1: Orbitcon Data Flow Diagram

Participants were asked to turn on their webcams so that they could see each other during the workshop.

After the introductory presentation, the system data flow diagram shown in Fig. 1 was introduced through screen sharing and explained by the product manager.

Then came the brainstorming phase. Participants received support handouts as they were not able to use the whiteboard and the size of the shared screen was limited. The step-per-element method was applied starting with the outer layers, focusing primarily on the width. Under the guidance of the facilitator, the team began to discuss threats using the STRIDE mnemonic for each element of the diagram.

Several problems arose during the creative threat discovery phase. Many participants turned off their webcams, and it became impossible to see if they were focused on the meeting or if their attention had shifted to something else. Active members experienced internet connection failures that impacted voice quality and overall user experience [9]. Some participants with experience in threat modeling recommended a different approach. As new ideas were encouraged during the brainstorming phase, these ideas were also noted, but diverted the attention of the contestants from the original track.

As a result of the collective brainstorming, twelve threats were identified. Since no time was reserved at the end of the workshop to triage bugs, these findings were not evaluated further, and no remedial action was suggested, nor recorded in Jira. It is important to note that during the workshop, one participant who did not actively participate in the brainstorming independently compiled a list of threats from 54 conclusions.

Workshop evaluation

At the end of the workshop, unstructured interviews were conducted with key workshop participants. In addition, the analysis was performed with reflection and abstraction as suggested by Vaishnavi et al. Several areas for improvement were found. Some of them refer to the preparation phase, while others refer to the workshop phase. Table 2 includes an assessment and suggested areas for improvement in preparation for the workshop.

Table 2

Assessment and areas for improvement - preparation stage

Element	Rating	Recommendations for Consideration and Improvement
List of Invitees	The number and skill set of people invited to the seminar was consistent with the theory. The management was overrepresented.	During the creative phase of threat detection, the presence of management can prevent some employees from having their say. Since management does not make decisions during the brainstorming phase, attendance should be optional. The presence of leadership is helpful during the bug triage phase when decisions about priorities and mitigation strategies need to be made.
Agenda invitation	It did its job well.	The use of brief reference material and small individual assignments could better guide participants' preparation efforts.
Format	The format of the online seminar was not ideal for brainstorming. It's hard to keep members. Difficulty reading body language and non-verbal communication. Whenever possible, online brainstorming workshops should be avoided.	Otherwise, the number of participants must be reduced. The use of a webcam should be mandatory. Motivational tools for active participation should be considered. for example, gamification.

The online conferencing platform	MS Teams has served this purpose well.	Company policy or best practices may affect which platform can be used. The features available in online conferencing tools are evolving rapidly, so it's a good idea to explore and experiment with them regularly.
Online drawing tool	Draw.io was satisfactory.	Key points to consider: whether the tool is cloud-based or standalone; supports online collaboration or not; has a threat modeling diagram library or not. The price may also influence the decision.
Structure and length	The length was reasonable. The structure should be reviewed.	The workshop can be aimed at exploring threats with a creative brainstorming method or sorting errors with the involvement of decision makers. Hybrid cases may not work as intended.
Create a chart	Create a data flow diagram of the system in advance to save time during the meeting.	However, this lessened the positive effect of collaborative charting. Charting the data flow together can be a good tool to break the ice for the group and help improve the overall understanding of the system. Also, it can help clarify issues or priorities for everyone.

A key takeaway from the preparation phase is that it is critical to assemble the right team based on the purpose of the meeting (brainstorming or sorting out bugs) and to clearly state goals and expectations [10].

The evaluation of the workshop and the main conclusions are shown in Table 3.

In addition, recommendations for review and improvement are provided for each finding [11].

Table 3

Evaluation and areas for improvement - workshop stage

Element	Rating	Recommendations for Consideration and Improvement
Opening presentation	It served its purpose.	The more experienced the team becomes in threat modeling, the less time is required for the introductory presentation. At this point, each participant should be asked to give a thirty second introduction, their role, their expectations, and their intended contribution to the workshop. This can increase the level of active participation during the session.
System Diagram Presentation	The explanation was good, but had a moderate effect.	Although the description of the system was well done, limited effects as explained in Table 3.
Brainstorming	This has had mixed results.	As described above, brainstorming through an online platform is challenging. Many factors can affect its outcome, for example, cultural characteristics, corporate culture, people who do not know each other, the involvement of management. This must be taken into account. Brainwriting can help overcome these barriers.
Method	The STRIDE Chosen method for each element did not work	If the participants include people with experience threat modeling, it is desirable to conduct a

	during the online brainstorming session.	preventive iteration with them before the workshop. This helps confirm that everyone is in agreement with the method.
Using the webcam	Didn't work at all.	If people choose to turn off their webcams, relevant motivational tools should be considered to change this behavior.
Technical infrastructure (Internet, microphone, speaker)	Although high-speed Internet access was widely available, there were some interruptions in the connection. Speakers and microphones have greatly impacted the user experience.	Another disadvantage of online brainstorming is that unexpected events may occur. Participants cannot join, the internet connection may become unstable, or someone's speakers may generate echoes. This is difficult to prevent or plan for.

During the workshop phase, it should be decided in advance whether the team can work more effectively through brainstorming or brainwriting [12]. As discussed above, this is a matter of culture and company culture, much like using a webcam all the time [13]. In addition, a structured brainwriting session can also help you avoid the inconvenience of potential technical issues.

4. Conclusion

This article discusses the modeling of information security threats for the terrestrial segment of space communications. A theoretical analysis of threat modeling is given, including the protection of terrestrial satellite systems. In the practical part, the threat modeling for the ground segment was described, the organization and evaluation of the seminar on threat modeling.

As a result of the work presented in this article, you should decide in advance whether the team can work more efficiently through brainstorming or brainwriting. It is a matter of culture and corporate culture, as well as the constant use of a webcam. In addition, a structured brainwriting session can also help you avoid the inconvenience of potential technical issues.

5. References

[1] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, A. Davis, Cyber Security in New Space: Analysis of threats, key enabling technologies and challenges, Survey Centre for Cyber Security, University of Surrey, Guildford, UK, 2022.

[2] A. S. Utegen, K. Moldamurat, M. Ainur, A. G. Amandykuly, S. S. Brimzhanova, Development and modeling of intelligent control system of cruise missile based on fuzzy logic, in: Proceedings of the 16th International Conference on Electronics Computer and Computation, ICECCO, 2021.

[3] M. Manulis et al., Cyber security in New Space, International Journal of Information Security 20 (2021) 287-311.

[4] K. Moldamurat, A. S. Utegen, S. S. Brimzhanova, D. M. Kalmanova, N. G. Yryskeldi, Development of a software simulator for small satellite swarm control, in: Proceedings of the 16th International Conference on Electronics Computer and Computation, ICECCO, 2021.

[5] N. Hillevi, P. Linnea, A multidisciplinary Analysis of Cyber Security in the Swedish Space Industry, Uppsala Universitet, 2022.

[6] A. K. Yemelyev, K. Moldamurat, R. B. Seksenbaeva, Development and Implementation of Automated UAV Flight Algorithms for Inertial Navigation Systems, in: Proceedings of the IEEE International Conference on Smart Information Systems and Technologies, SIST, 2021, 9465965.

[7] B. P. Bela, Cyber Security in the Space Domain, JAMK University of Applied Sciences, 2021.
[8] A. Kyzyrkanov, S. Atanov, S. Aljawarneh, Coordination of movement of multiagent robotic systems, in: Proceedings of the 16th International Conference on Electronics Computer and Computation, ICECCO, 2021
[9] P. James, Securing New Space: On Satellite Cyber-Security, Wolfson College, 2021.
[10] A. K. Kereyev, S. K. Atanov, K. P. Aman, Z. K. Kulmagambetova, B. T. Kulzhagarova, Navigation system based on bluetooth beacons: Implementation and experimental estimation, Journal of Theoretical and Applied Information Technology, 98.8 (2020) 1187-1200.
[11] D. Yergaliyev, A. Tulegulov, A. Zhumabayeva, A. Yussupov, A. Zhauyt, Study of stress-strain state of the roller conveyor, Metalurgija 61.2 (2022) 347–350.
[12] A. Melnichuk, E.A. Kuzina, N.K. Yurkov, Methods and means for countering unmanned aerial vehicles, in: Proceedings of the International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM, 2020, 9112082.
[13] Kh. Moldamurat, S. Akhmejanov, K. Kariyeva, Zh. Omarov, D. Kalibekov, N. Sayasat, Design and optimization of the parameters of a hybrid unmanned aerial vehicle in the SolidWorks complex, in: Proceedings of the International Conference on Smart Information Systems and Technologies, 2022.