Cybersecurity Risk Assessment Report:

BYU-MAYANSAT Cube Satellite

Team Spaceforce

Jona Monette, Matt Lemmon, Angela Milova, Kaden McLinn, Brooke Brewer

April 2024

**Executive Summary**

This report conveys our (Cybersecurity capstone team Spaceforce) assessment of cyber risk associated with the project undertaken by electrical engineering capstone team 38. Team 38’s objective was to have prepared a cube satellite for launch in late 2024 NLT this April. Our objective was to advise them on security concerns, licensing restrictions, and to evaluate any cyber risk associated with their decision making. Unfortunately many of the critical cyber related decisions were left to the last minute leaving little room for a thorough assessment and mitigation of risk, but team Spaceforce was able to identify several risks through analysis of the cubesat platform from Endurosat, the ground station computer, and

<#todo once finished, redo with chat>

**Introduction**

The purpose of this cyber risk assessment report is to meticulously evaluate and address the various cybersecurity risks associated with a groundbreaking student-led satellite project at Brigham Young University (BYU). This ambitious endeavor, driven by a dedicated team of cybersecurity majors, aims to construct, launch, and manage a satellite, marking a significant milestone in the university's foray into space exploration and technology. The focal point of our cybersecurity efforts centers on ensuring the robustness and integrity of the ground station computer system, which serves as the critical communication link between the team and the satellite.

The satellite project introduces a complex array of cyber risks that could potentially compromise the mission's success and safety. Recognizing the pivotal role of cybersecurity in this context, our team has embarked on a comprehensive risk assessment to identify, evaluate, and mitigate potential threats. This initiative is crucial for safeguarding the satellite and ground station against cyberattacks, operational failures, and compliance violations, thereby securing the mission's objectives and our stakeholders’ investment in this venture.

Given the stakes of the project, our risk assessment extends beyond conventional cybersecurity challenges, encompassing unique threats associated with space operations, such as unauthorized command/control, jamming, battery draining attacks, and regulatory compliance failures. These challenges underscore the importance of a rigorous and adaptive cybersecurity strategy tailored to the specific needs and vulnerabilities of the satellite mission.

As we navigate through the complexities of cybersecurity in space technology, this report serves as a foundational document outlining our strategic approach to managing cyber risks.

By detailing our methodology, findings, and recommendations, this report aims to provide a clear and actionable roadmap for enhancing the cybersecurity posture of the satellite project. It is designed to inform and guide the project team and stakeholders ensuring that cybersecurity considerations are integral to the project's planning, execution, and future management.

**Methodology**

The methodology employed in this cyber risk assessment is designed to systematically identify, evaluate, and propose measures to mitigate cybersecurity risks associated with the BYU student-led satellite project. Given the project's focus on constructing and managing a satellite, including the crucial ground station computer, our approach integrates practical cybersecurity practices, compliance efforts, and collaborative insights from interdisciplinary teams. This section outlines the steps taken to ensure a thorough and effective cyber risk management process.

**Risk Identification**

Our first step in our methodology was to identify risks of the system, and in order to do that we needed to learn how the system functions and what regulations we would need to comply with. We identified regulatory requirements and some common satellite specific risks as well as other common risks to normal computers like the ground station computer. Meeting with the hardware team, we learned the components of the satellite and discovered potential avenues of attack through them. Conducting a vulnerability scan on the ground station computer was our final round of risk identification.

**Risk Assessment**

Following the identification of potential risks, the next step in our methodology was the thorough assessment of these risks. This phase involved evaluating the identified risks in terms of their likelihood of occurrence and potential impact on the project. Utilizing a combination of the information gleaned from our initial hardware team collaboration and the insights from our vulnerability assessment of the ground station computer, we were able to prioritize the risks based on a structured criteria. This evaluation took into account factors such as the severity of potential damage, the exploitability of identified vulnerabilities, and the criticality of affected system components. The risk assessment phase was instrumental in quantifying and qualifying the nature of the cyber threats we faced, enabling us to develop a prioritized list of risks that warranted immediate attention and mitigation strategies.

**Reporting + Recommendations**

The final phase of our methodology culminated in the synthesis of our findings into this detailed report, which not only outlines the identified risks and their assessments but also proposes specific recommendations for mitigating these risks. This report serves as a strategic document, offering actionable insights and tailored recommendations aimed at enhancing the cybersecurity posture of the satellite project. Our recommendations are based on best practices in cyber security and are designed to address the unique vulnerabilities and threats identified through our comprehensive assessment process. Key recommendations include the implementation of secure configuration of hardware modules, regular software updates and vulnerability patches, and the development of contingency plans for critical systems. Through this reporting and recommendation phase, we aim to provide a clear and actionable path forward to mitigate the cyber risks associated with the satellite project, ensuring its security and compliance throughout its lifecycle.

**Findings**

Our team identified, assessed and prioritized various weaknesses in the system that may pose a threat to the project. Our findings are as follows.

**Identified Risks**

This section presents a comprehensive catalog of the cybersecurity risks identified during our assessment process. These risks, emerging from technical vulnerabilities, operational challenges, and external threats, highlight potential weaknesses within the satellite project's cyber infrastructure. Detailed herein are the various threat vectors that could potentially compromise the integrity and functionality of both the satellite and the ground station.

**Threat Vector #1 – Ground Station**

**Ground station computer corruption/crash**

Loss of ground station computer without a backup would lead to the satellite being orphaned. Losing control of satellite compromises mission objectives.

**Ground station unauthorized remote access**

This would enable full unauthorized control over the satellite. Control over the satellite would be lost.

**Inability to control satellite from ground station computer**

This could be due to unexpected errors in the software hardware is developing. We could still launch the satellite in this case, but we would have no access to it once it’s in space. Lacking control of the satellite compromises mission objectives.

**Threat Vector #2 – Satellite Computer**

**Unauthorized Commands**

This could happen perhaps through a replay attack, known ciphertext attack, man in the middle attack. Losing control of satellite compromises mission objectives.

**Jamming (Interference)**

Satellite control could be compromised by an attacker decreasing our signal-noise ratio. Loss of satellite control compromises mission objectives.

**Threat Vector #3 – Ham Payload**

**Battery Draining Attacks**

An attacker might overload the **ham repeater payload** by requesting lots of data / repeated radio, potentially straining the power system. This would lead to a dead satellite.

**Threat Vector #4 – Internal**

**Malicious Insider Threat**

Authorized individual could use privileges to send malicious commands to satellite, shut down services, etc. There is a large group with access to this ground station computer that have no direct tie to the MAYANSAT project. Access control is not currently set up to protect from insider threats.

**Human Error**

Authorized users without any malicious intent opening malicious attachments, downloading malicious software, etc.

**Threat Vector #5 – Social Engineering**

**Phishing**

Phishing can compromise of team workstations could lead to complete loss of project data. Phishing can also lead to compromise of secrets/credentials or confidential project data.

**Tailgating**

Malicious actor might follow authorized individual into CB 505 room, giving physical access to ground station, possibly leading to loss of control or compromise of secrets.

**Threat Vector #6 – Regulatory Compliance Failure**

**Fail to license with FCC / IARU in time**

Without confirmed approval from the government, launching our satellite would not be legal. Failure to legally launch the satellite compromises mission objectives.

**Impact and Likelihood Assessment**

Following the identification of potential risks, this section delves into a systematic evaluation of each risk in terms of its likelihood of occurrence and the extent of its potential impact on the project. We have given a score for each item’s impact level and its likelihood level, combining to indicate criticality. This assessment provides perspective on the severity of the identified risks, guiding the prioritization process by highlighting the threats that pose the greatest danger to the project's success and security.

**1. Unauthorized command/control of satellite**

- Probability: 4 – Recent cons and CTFs like the Hack-a-sat competition have proven even military grade satellites vulnerable to attack. Attacks on spacecraft may be increasing in popularity due to this fact.

- Impact: 5 - Unauthorized commands could lead to the satellite deviating from its intended orbit, altering its trajectory, or disabling critical systems, compromising the mission objectives. It also has Economic loss if losing control of the satellite and need to start the project all over.

**2. Battery Draining Attacks**

- Probability: 2 – While there is data to support that this is possible, not much is known regarding the hardware limitations of the satellite (if fully draining it is even possible). Threat actors also do not have much to gain by specifically attacking via battery draining.

- Impact: 3 - Continuous requests for data or repeated radio transmissions can strain the satellite's power system. The inability to power essential systems results in mission failure, affecting the satellite's overall objectives.

Need to determine the capacity, recharging, if shuts down if it can recharge and reboot

**3. Phishing**

- Probability: 3 – Phishing is a common attack that everyone is susceptible to. If a particular phishing email contains ransomware or other destructive malware, important data key to the project might be destroyed or secrets for authorized access might be exposed.

- Impact: 5 - Successful social engineering, such as phishing, may lead to the extraction of sensitive information related to satellite control. Compromised information could facilitate unauthorized access to satellite control systems.

**4. Ground Station Computer Corruption/Crash**

- Probability: 3 - Hardware is not new, susceptible to component failure or hard drive corruption. Will fail within next few years.

- Impact: 5 - Loss of the ground station computer may result in the satellite being orphaned, with no means of communication or control.

**5. Ground station unauthorized access (Remote/physical access)**

- Probability: 5 - due to the persistent and evolving nature of cyber threats, malicious actors may attempt to exploit vulnerabilities in software, network protocols, or human factors to gain unauthorized access. Physical breaches, though less common, remain a risk as well.

- Impact: 5 - Unauthorized access to the ground station provides full control over the satellite. This scenario has a critical impact as it allows for complete, unauthorized manipulation of the satellite's functions.

**6. Malicious Insider Threat**

- Probability: 1 – Not many people outside of our major know of this project. Additionally, our satellite is not going to be holding valuable information, so the reasons to attack it are slim.

- Impact: 4 - An insider with authorized privileges could pose a serious threat by sending malicious commands, shutting down services, or otherwise compromising the satellite's mission.

**7. Human Error**

- Probability: 3 – Some level of human error will always be likely, but we will be checking each other’s work at every stage to reduce the chances of this affecting us negatively.

- Impact: 3 - A member of the team has the ability to make a mistake that could compromise the mission, which is why we all check each other’s work.

**8. Tailgating**

- Probability: 1– Not many people know about that room or what’s in it. The room is small and often very quiet, so it would be fairly easy to notice someone come in after another.

- Impact: 4 - Someone following us into the room could pose a security risk, but once infiltrated, an attacker would need the skills to bypass ground station authentication.

**Risk Prioritization**

Building on the insights gained from the risk impact and likelihood assessment, this segment prioritizes the identified risks. By arranging the risks in order of their criticality, this prioritization aids in focusing mitigation efforts on the most significant threats first, ensuring efficient allocation of resources and strategic planning to address the vulnerabilities most likely to impact the project adversely.

**Priority Rankings:**

1. **Ground Station unauthorized access (Remote/physical access)**
2. **Unauthorized command/control of satellite**
3. **Phishing**
4. **Ground Station Computer Corruption/Crash**
5. **Human Error**
6. **Battery Draining Attacks**
7. **Malicious Insider Threat**
8. **Tailgating**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Identified Risk** | **Component** | **Likelihood Score** | **Impact Score** | **Risk score** | **Mitigation** |
| Ground Station Unauthorized Access / Control | GS | 5 | 5 | 25 | Vulnerability scan, remediation, implementation of access control |
| Unauthorized control | Satellite | 4 | 5 | 20 | Further analysis needed; encryption; session keys |
| Phishing | Data, team hardware | 3 | 5 | 15 | Training |
| Ground Station Disaster | GS, data | 3 | 5 | 15 | Backup drive |
| Human Error | All | 3 | 3 | 9 | Training |
| Battery Drain Attacks | Sat | 2 | 3 | 6 | Further analysis needed |
| Insider Threat | All | 1 | 4 | 4 | Compartmentalization Policy |
| Tailgating | GS, data | 1 | 4 | 4 | Training |

**Recommendations**

**Mitigation Recommendations**

Implement different accounts on the computer for different purposes (PICS vs MAYANSAT)

Verify encryption, strong assumption but need to verify // where in the system architecture is the encryption and what type is it

Continue door code rotation

Implement the backup solution using this link:

Need to continue researching battery drain attack and if it is applicable

Need to continue researching buffer overflow or other injection through ham payload

Need to continue researching ways to take down ham payload

Need to continue researching ways to mitigate satellite accepting commands from non authorized sources, we didn’t do much regarding that

Patch the vulnerabilities, misconfigurations mentioned

You guys need to fix these misconfigurations, upgrade fedora?

#todo feed this into chatgpt

**Monitoring + Incident Response Plan**

#todo Mention watching for IOCs and using the IRP we have included separately

**Conclusion + Additional Recommendations**

Do a full, intensive code review to really understand what is going on

Conduct a penetration test

Identified stretch goals: didnt get to them for this reason (not bc hardware team sucked) more in depth than thought, didn’t have time