Threat Modelling

# AstroDev

1. What are we building – A system that allows grounds communications and computers on spacecrafts to operate with minimal disruption
2. What can go wrong – Signals and messages between the ground stations and the spacecraft can be intercepted by unwanted parties
3. What are we going to do about it – Ensure security within the communications, keeping information and confidential information private
4. Did we do a good job –

# AstroDev Risk Treatment Plan

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Risk  ID | Risk  Description | Risk  Treatment | Likelihood | Impact | Impact Total | Status |
| 1 Changing research data (Tampering) | Researchers could change the data giving incorrect results | Only give the right level of permissions depending on their type of work | 2 | 3 | 5 | Mitigated |
| 2 Account access (Spoofing) | Gain access to an account on ground control potentially giving the attack access to the entire network. This can also cause the incorrect data to be sent to the spacecraft leading to risk of life among the astronauts. | Multi-step verification for login, including use of biometrics | 3 | 5 | 8 | Mitigated |
| 3 Network access (Information disclosure) | Access to the credential database would give an attacker unlimited access to the usernames, passwords, and administrative levels of a user. | Encrypt all data for the database | 3 | 4 | 7 | Mitigated |
| 4 Account access (Spoofing) | Access to the user account can allow an attacker to alter research data within a system. | Ensure that the level of permissions that a user has is just enough for them to get their work done. Make the database view only for most users and only in the areas they need access to. Train users to spot spoofing emails | 2 | 1 | 3 | Mitigated |
| 5 Information tampering (Tampering) | If the data is tampered with in this database, it can lead to ground control to send back the spacecraft the wrong information. This could lead to the lethal outcomes to astronauts. | Make the data read only to all users, and have very few system admins. Encrypt all data in the database. | 4 | 4 | 8 | Mitigated |
| 6 Changing adjustment data  (Tampering) | Access to the credential database would give an attacker unlimited access to the usernames, passwords, and administrative levels of a user. | Encrypt all data for the database | 3 | 3 | 6 | Mitigated |
| 7 Access to user info (Information disclosure) | Access to this database can allow an attacker to see the privilege of accounts as well as usernames and passwords which will allow further access to all levels of an organisation | Hash passwords, multi-level authentication, encrypt network | 3 | 5 | 8 | Mitigated |