AstroDev Threat model

Owner: G:01
Reviewer: G:01
Contributors:
Date Generated: Sat Nov 16 2024

Executive Summary

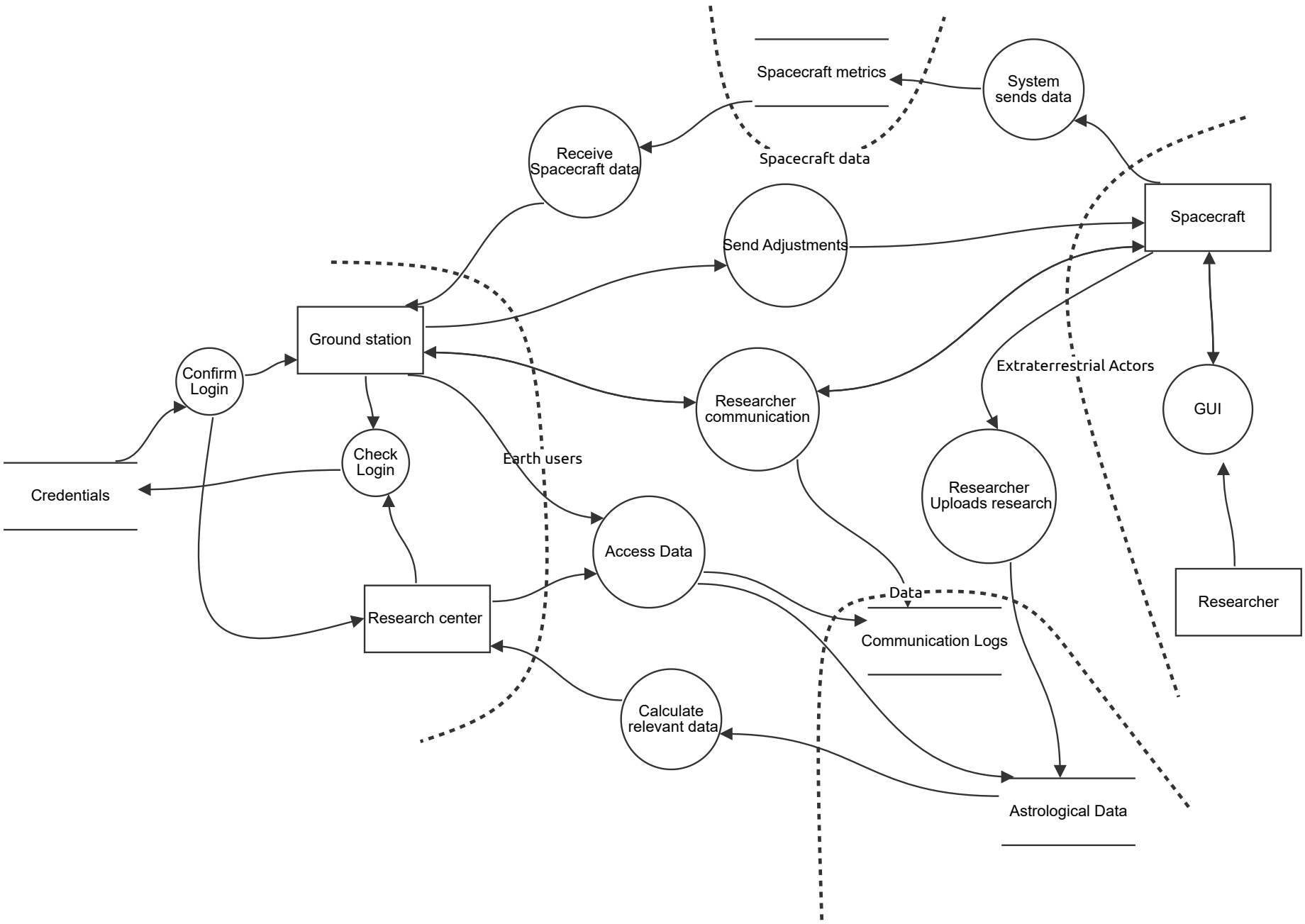
High level system description

A communication system between a spaceship and ground control, where messages are able to be sent. This includes large datasets with astrological information from missions.

Summary

Total Threats	19
Total Mitigated	19
Not Mitigated	0
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

Threat model



Threat model

Spacecraft (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Flow (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Ground station (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
21	Malicious User Gaining Access	Repudiation	Medium	Mitigated	7	Data can be altered or leaked by a user.	All users need multi-layered authentication to access their accounts, logs of all activity will be kept as a security measure

Astrological Data (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
40	Alteration of research data	Tampering	Low	Mitigated	3	Data can be altered in the dataset, this could lead to incorrect information provided for the research projects conducted by AstroDev.	No researcher will have direct access to this dataset, and will only be able to see the data through their GUI.
41	Staff make research changes without ownership	Repudiation	Medium	Mitigated	3	Data can be added or removed from the dataset which is incorrect leading to errors in the research	Logs will be kept of all access to the dataset

Research center (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
23	Malicious User Access the data	Repudiation	Low	Mitigated	3	Research data can be manipulated or changed maliciously by a user.	Logs will be kept every time the data is altered.

Spacecraft metrics (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
15	Denial of Service	Denial of service	High	Mitigated	5	The data store may be inundated with packets which can cause the database to miss or be unable to receive data from the spacecraft. This can lead to the spacecraft to be left to drift off-course which could have lethal consequences	Implement a web application firewall to only approve data from only specific IPs.
16	Database manipulation	Tampering	High	Mitigated	7	The data could be manipulated in the database leading to the wrong metrics of the spacecraft which could cause disasterous consequences.	Ensure that data cannot be changed in this database, only written and read. Also ensure that the system is responsible for removal of old data and not an individual.
17	Unauthorised changes	Repudiation	High	Mitigated		The data could be deleted or altered if everyone has access to the database when they are not meant to be.	Ensure that there is only a handful of users that can do more than read from the database that need access to it and only those who are trusted.

Researcher
Uploads research (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	Data tampering	Tampering	Low	Mitigated	3	Data could be altered during the data transfer leading to the incorrect data being input.	Data should be encrypted and verified through the correct IP logs.

System
sends data (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
13	Data tampering	Tampering	High	Mitigated	6	Data could be manipulated during transmission leading to incorrect data being saved into the database. This could lead to spacecraft metrics being adjusted wrong causing the spacecraft to be sent off-course	Encrypt all data with multi-layered encryption. The data should also be only accepted from accepted IPs and with the correct authorisation codes.

Researcher (Actor)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Calculate
relevant data (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Receive
Spacecraft data (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
18	Data altered during transfer	Tampering	High	Mitigated	6	Data could be manipulated during the data transfer, this can lead to the wrong values being transferred causing the calculations being wrong.	Data needs to be compared to the database, if the data does not match it needs to be flagged for review.

GUI (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Send Adjustments (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
20	Data tampering	Tampering	Medium	Mitigated	5	Data can be intercepted by a third party and manipulated.	Encrypt data and verify data from other ground bases.

Researcher communication (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
35	Spoofed communications	Spoofing	Medium	Mitigated	4	An attacker could intercept, alter, or prevent information transmission and manipulate it.	All network communications must be encrypted and on a closed network. It must also be verified through logs

Credentials (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
26	Credentials altered	Tampering	High	Mitigated	7	The user credentials could be altered by an external party, this could lead to the data store having new users added with admin privileges which could have massive consequences. Users could also have access to the dataset and alter usernames or passwords.	The database should be admin access only, all data should be encrypted and kept on a closed network and standard users should not be able to see the database.
27	Database leak	Information disclosure	High	Mitigated	8	The data from the dataset could be leaked leading to huge security breaches across all of the networks.	Data should remain encrypted with privileged users being able to see it.

Check Login (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
25	Data interception	Information disclosure	High	Mitigated	9	Data can be intercepted during the login of the device. This could lead to account information being accessed and then lead to the affected accounts being access.	All login data needs to be encrypted. The database should only be on a closed network to reduce the probability of an external attack.
33	Wrong user privileges	Elevation of privilege	High	Mitigated	8	Users could have higher levels of access than they require, leading to altering of the data.	Users are given minimum access privilege to only have access to the correct data. Login information is encrypted during the login process.

Confirm Login (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Communication Logs (Store)

Number	Title	Type	Priority	Status	Score	Description	Mitigations
36	Alteration of communication logs	Tampering	Medium	Mitigated		Logs could be modified by an external or internal entity, this could lead to incorrect mission logs should an issue occur.	Only authorised personnel can access communication logs with minimum access privileges. The logs cannot be changed even by admins and can only read or delete logs.

Number	Title	Type	Priority	Status	Score	Description	Mitigations
37	Changes to comm logs	Repudiation	Medium	Mitigated	4	Communication logs may be altered or deleted by staff, and the user may deny having done so.	Logs will be kept whenever a user accesses or changes the data store in any way.
39	Sensitive information may be leaked	Information disclosure	Medium	Mitigated	4	Sensitive information could be leaked from the communication logs. Due to the type of operation at AstroDev, information could be highly sensitive or top secret.	Only authorised personnel should have access to the dataset and should have the relevant security clearance.

Access Data (Process)

Number	Title	Type	Priority	Status	Score	Description	Mitigations