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

Defence Ventures

1. What are we building – ShieldX: A secure defence software that benefits both military and civilian sectors, where it acts as a solution of providing barriers of security for defence organisations' systems.

2. What can go wrong – Unknown threats that aren't registered with ShieldX can slip through and cause problems with organisations' systems.

3. What are we going to do about it – Regularly record newfound threats to provide solutions and prevent attacks on systems

4. Did we do a good job -

Defence Ventures Risk Treatment Plan

Risk ID	Risk Description	Risk Treatment	Likelihood	Impact	Impact	Status
1 Spoofing attack (Spoofing)	An attacker could send a phishing email or a spear phishing attack to try and gain access to the system	The management system will recognise this attack and filter it out sending a report to a user.	3	4	7	Mitigated
2 Wrongful request of data (Information disclosure)	An attacker may try and request data from the database when not having permissions to do so, to	Monitor where the user is requesting data from, if its not an approved IP cancel the request. Also ensure that it	3	3	6	Mitigated

	gain privileged information	is from an employees account				
3 Access to too much information (Elevation of privilege)	A user may access more data than they need allowing them to have too much control over a system	Give a user the minimum amount of permissions to be able to do their job	2	3	5	Mitigated
4 Account breach (Spoofing)	The user could possibly modify the system if they have enough privileges.	Appropriately authorise the user and introduce integrity checks (such as Hashes and Digital Signatures)	4	5	9	Mitigated
5 Manipulation of data (Tampering)	An attacker abuses the application to perform unintended updates to a database.	Implement appropriate authorisation measures and introduce integrity checks, such as Hashes	3	3	6	Mitigated
6 DDOS attack (Denial of service)	Attacker launches a denial of service attack preventing the network from being used	Network monitoring to ensure packets are from an authorised user	1	2	3	Mitigated
7 Repudiation attack (Repudiation)	An attacker manipulates logs to cover their actions.	Ensure appropriate authorisation is put in place, check audit logs and timestamps	2	3	5	Mitigated