DREAD Analysis | Compromising a Medical Mannequin

Case #	Case Description	Mitigation Plan
Case A	Input data from the administrator (spoofed) is compromised towards the Mannequin	- Use Biometric or 2 Factor Authentication to double check the identity of the administrator accessing the device. - Use timer based solution to ensure transactional authentication.
Case B	Reliability of OEM (Original Equipment Manufacturer) via upgrades OTA (Over The Air)	- Sequential upgrade so that process uses the md5 hash of the previous image to flash the new image. - Hardware combination to factory reset(ability to roll-back in case of failure) to ensure device consistency
Case C	DoS attack during emergency incident or critical examination	- Design the ability to override and hijack the system in case of an emergency by employing physical least proximity based solution.
Case D	Intercept personal information with Man in the Middle attack during information transfer	- Avoid transfer in plain text by implementing tunnel based solution (like IPSec etc) to encrypt communications.

Case #	Damage potential	Reproducibility	Exploitability	Affected users	Discoverability	Total	Rating
Case A	3	2	2	1	2	13	**High Risk**
Case B	3	1	1	3	1	9	**Medium Risk**
Case C	1	3	3	3	3	13	**High Risk**
Case D	2	2	3	3	2	12	**High Risk**

Risk Rating Matrix	
12 to 15	**High Risk**
8 to 11	**Medium Risk**
5 to 7	**Low Risk**

Group 2: Lukasz, Raquel, Spiros, Vaibhav