Compromising a Medical Mannequin

STRIDE AND DREAD

STRIDE

Spoofing	AAA – Authentication, Authorisation, Accounting Failure to authenticate the programming unit creates an opportunity for the implanted device to receive parameter changes from any unit, both malicious and legitimate.
Tampering	The lack of authentication and access control of the programming unit creates a vulnerability where a malicious actor can modify the operational parameters of the implantable medical device. The threat source could be a competitor trying to discredit the reputation of the manufacture of the device.
Repudiation	AAA – Authentication, Authorisation, Accounting The absence of logging transactions performed on the medical device creates an opportunity for non-repudiation of maliciously tampering with the medical device by the disgruntled medical staff.
Information disclosure	Disclosure of data exchanged between the programming unit created an opportunity for violation of confidentiality—the communication channel between the nodes needed to be encrypted to prevent access to data through packet sniffing.
Denial of service	AAA – Authentication, Authorisation, Accounting Non-authentication of the programming unit allows for any other unit to manipulate the implanted device. Thus a malicious actor may shut down the device; thus, denying service to the person with the device implanted.
Elevation of privilege	AAA – Authentication, Authorisation, Accounting The threat actor could implement the AAA system, create an account with elevated privileges and deny everyone access to the system.

DREAD

Threat	D	R	E	A	D	TOTAL	RATING
The threat actor obtains access to confidential information by using a packet sniffer to monitor the network traffic between the programming unit and the implanted device.	3	3	2	3	2	13	High
Threat actor switching off the implanted device by obtaining a malicious operating unit since the device does not authenticate the operating unit.	3	3	1	3	1	11	High