As the utilisation of implantable medical devices expands and becomes an increasingly vital component of healthcare, securing medical devices becomes essential (Maple, 2017).

Threat Modelling :

STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of service, Elevation of privilege) methodology can be used to classify security threats against implantable medical devices(IMD) (Núñez, 2017). The relationship between the threat and the security service attacked with a focus on the IMD is as follows;

Security Service	Threat to the security service
Authentication	Spoofing
Integrity	Tampering
Nonrepudiation	Repudiation
Confidentiality	Information Disclosure
Availability	Denial of service
Authorisation	Elevation of privelege

Threat identification to the IMD using STRIDE methodology (adapted from (Núñez, 2017) **:**

Security Service	Threats	
Authentication	Impersonate the programmer. Impersonate the IMD. Impersonate the external device	Spoofing
Integrity	Patient data tampering Malicious input Modify communication on the wireless network	Tampering
Non-Repudiation	Delete access logs Repeated access attempts	Repudiation
Confidentiality	Disclose medical information Determine the type of IMD Disclose the existence of the IMD Track the IMD	Information Disclosure
Availability	Drain the battery of the IMD Interfere with the IMD communication capabilities Flood IMD with data	Denial of Service
Authorisation	Reprogram the IMD Update the therapy on the patient Switch-off the IMD	Elevation of privilege

Wireless Network Security :

Communication over the wireless network has become integral to modern implantable medical devices(IMDs). Thus, IMD devices inherit the existing security risk of wireless networks. Wireless networks have vulnerabilities that, if not mitigated, can be exploited to compromise the confidentiality of the data exchanged with the IMDs or to send maliciously unauthorised instructions to the IMD and tamper with the operational functions of the device to cause harm to the patient (Gollakota et al., 2011).

Securing the data exchanged and the wireless network the data exchange is on can be approached in the parts - secure channel establishment, physical security, and access control. The distribution of cryptographic keys between the networks node in the wireless network can create a secure network channel, and such a channel prevents (i) eavesdropping and traffic analysis by providing confidentiality(encryption) and (ii) man in the middle attack or spoofing attack (Venkatasubramanian et al., 1993). Following the principle of implementing multiple layers of security, an additional layer of security can be provided by constructing authorisation primitives based on access control conceptual elements such as role-based access control(RBAC).

References:

Gollakota, S. *et al.* (2011) 'They can hear your heartbeats: Non-invasive security for implantable medical devices', *Computer Communication Review*, 41(4), pp. 2–13. doi: 10.1145/2043164.2018438.

Maple, C. (2017) 'Security and privacy in the internet of things', *Journal of Cyber Policy*, 2(2), pp. 155–184. doi: 10.1080/23738871.2017.1366536.

Núñez, C. C. (2017) 'Cybersecurity in Implantable Medical Devices'.

Venkatasubramanian, K. K. *et al.* (1993) 'Interoperable Medical Devices', *IEEE Transactions on Information Theory*, 39(3), pp. 903–912. doi: 10.1109/18.256498.