STRIDE MODEL

Spoofing: Attacker could impersonate as the medical controller for the pacemaker device, from which the attacker could utilize elevated privilege for an attack.

Tampering: Possibility of tampering with patient data. Attacker could make malicious inputs such as sending excessive electrical signals to the heart.

Repudiation: Attackers could find the access logs for every operation performed on/by the pacemaker and either alter or delete log events to prevent any evidence of an attack.

Information disclosure: Attackers could read data being transferred between the pacemaker and whatever machine responsible for monitoring the pacemaker, especially if the data is not encrypted. Just the presence of the pacemaker being detected could also be a privacy issue.

Denial of Service: Attackers could flood the frequency that the pacemaker is using to prevent communication between the pacemaker and the medical controller.

Elevation of privilege: Attackers could perform operations that normally would only be authorized by medical professionals such as altering the values in the pacemaker like voltage and current levels or possibly even shut off the pacemaker entirely.

PROBLEM DOMAIN

The problem domain I am working on is the security of patient devices, particularly internal devices like pacemakers that are crucial for patient health. Protecting patient device function and patient data from cyberattackers will become more important as more patient devices obtain connectivity to the internet. An effort should be made to ensure that communication between devices are encrypted and hidden with authentication measures to prevent cyberattackers from exploiting hospital and patient security (manipulating/stealing data, disrupting devices, etc.).