The data transmission between the implantable medical device(IMD) and the IMD programming unit is unencrypted, and this allowed subjects to get unauthorised access to sensitive information. Halperin et al.(2008) indicated that they were able to modify the device's operational parameters. The lack of authentication and access control of the programming unit creates a vulnerability, and such vulnerability is exploitable by launching a denial of service attack on the implanted device (Rathore et al., 2017).

Data encryption and authentication mechanisms should be employed to conceal data exchanged by the implanted device and the programming unit, thus protecting the confidentiality of the data. Authenticating the programming unit will protect the implanted device against denial of service by ensuring that only an authorised unit can modify the device's operational parameters (Rathore et al., 2017). However, due to their processing requirement, security protocols such as cryptography and hashing will take a toll on the battery powering the implantable device and cause it to drain more quickly.

Wi-Fi Protected Setup(WPS) was used to authenticate connections to the network access point. One of the authentication method used by WPS is the manual input of an eight-digit extended PIN code. This method should yield 10^8 (100.000.000) possible codes. However, WPS uses the last digit of the code as a checksum, and the first four digits are validated separately from the last three digits. Thus performing a brute force attack will take $10^4 + 10^3$ (11000)attempts. This result in one PIN validation taking 1.3 seconds and taking a full brute force attack for 3.06 hours to go through all possible combinations(Kalniņš, Puriņš and Alksnis, 2017).WPA2-802.1X(WPA2-Enterprise) is one of the authentication methods to be used instead of WPS. Devices must supply a digital certificate issued by a trusted certification authority as a form of authorised credentials to participate in the 802.XX network(*Enterprise wireless LAN security: 802.11 and seamless wireless roaming*, 2009).

References:

Enterprise wireless LAN security: 802.11 and seamless wireless roaming (2009). Available at: https://searchnetworking.techtarget.com/tutorial/Enterprise-wireless-LAN-security-80211-and-seamless-wireless-roaming [Accessed: 12 May 2021].

Halperin, D. et al. (2008) 'Pacemakers and Implantable Cardiac Defibrillators - Security', *IEEE Symposium on Security and Privacy*, pp. 1–14. Available at: https://www.secure-medicine.org/hubfs/public/publications/icd-study.pdf.

Kalniņš, R., Puriņš, J. and Alksnis, G. (2017) 'Security Evaluation of Wireless Network Access Points', *Applied Computer Systems*, 21(1), pp. 38–45. doi: 10.1515/acss-2017-0005.

Rathore, H. et al. (2017) 'A review of security challenges, attacks and resolutions for wireless medical devices', *2017 13th International Wireless Communications and*

Mobile Computing Conference, IWCMC 2017, (June), pp. 1495–1501. doi: 10.1109/IWCMC.2017.7986505.